

Caveats

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats, and only select severity 3 caveats are included in the caveats document.

Because Cisco IOS Release 12.0S is based on Cisco IOS Release 12.0, many caveats that apply to Cisco IOS Release 12.0 will also apply to Cisco IOS Release 12.0S. For information on severity 1 and severity 2 caveats in Cisco IOS Release 12.0, see the [Caveats for Cisco IOS Release 12.0](#) document located on Cisco.com.



Note

If you have an account on Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to [Cisco.com](http://www.cisco.com) and click **Technical Support: Tools & Resources: Bug Toolkit**. (The Bug Toolkit is listed under Troubleshooting.) Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl. (If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.)

These caveats are documented in the following format:

- Symptoms: A description of what is observed when the caveat occurs.
- Conditions: The conditions under which the caveat has been known to occur.
- Workaround: Solutions, if available, to counteract the caveat.

The caveats section consists of the following subsections:

Cross-Platform Release Notes for Cisco IOS Release 12.0S, Part 3: Caveats for 12.0(33)S11 through 12.0(30)S

- [Resolved Caveats—Cisco IOS Release 12.0\(33\)S11, page 359](#)
- [Resolved Caveats—Cisco IOS Release 12.0\(33\)S10, page 360](#)
- [Resolved Caveats—Cisco IOS Release 12.0\(33\)S9, page 364](#)
- [Resolved Caveats—Cisco IOS Release 12.0\(33\)S8, page 367](#)
- [Resolved Caveats—Cisco IOS Release 12.0\(33\)S7, page 369](#)
- [Resolved Caveats—Cisco IOS Release 12.0\(33\)S6, page 379](#)
- [Resolved Caveats—Cisco IOS Release 12.0\(33\)S5, page 397](#)
- [Resolved Caveats—Cisco IOS Release 12.0\(33\)S4, page 398](#)
- [Resolved Caveats—Cisco IOS Release 12.0\(33\)S3, page 399](#)
- [Resolved Caveats—Cisco IOS Release 12.0\(33\)S2, page 425](#)
- [Resolved Caveats—Cisco IOS Release 12.0\(33\)S1, page 443](#)
- [Resolved Caveats—Cisco IOS Release 12.0\(33\)S, page 469](#)
- [Open Caveats—Cisco IOS Release 12.0\(33\)S, page 471](#)

- [Resolved Caveats—Cisco IOS Release 12.0\(32\)S15, page 476](#)

- [Resolved Caveats—Cisco IOS Release 12.0\(32\)S14, page 484](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(32\)S13, page 489](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(32\)S12, page 493](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(32\)S11, page 508](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(32\)S10, page 521](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(32\)S9, page 532](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(32\)S8, page 554](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(32\)S7, page 571](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(32\)S6, page 581](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(32\)S5, page 596](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(32\)S4, page 605](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(32\)S3, page 619](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(32\)S2, page 623](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(32\)S1, page 643](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(32\)S, page 645](#)
-

- [Resolved Caveats—Cisco IOS Release 12.0\(31\)S6, page 735](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(31\)S5, page 743](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(31\)S4, page 753](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(31\)S3, page 764](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(31\)S2, page 781](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(31\)S1, page 792](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(31\)S, page 820](#)
-

- [Resolved Caveats—Cisco IOS Release 12.0\(30\)S5, page 877](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(30\)S4, page 898](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(30\)S3, page 914](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(30\)S2, page 937](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(30\)S1, page 938](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(30\)S, page 962](#)
-

Cross-Platform Release Notes for Cisco IOS Release 12.0S, Part 4: Caveats for 12.0(29)S1 through 12.0(27)S

- [Resolved Caveats—Cisco IOS Release 12.0\(29\)S1, page 1031](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(29\)S, page 1033](#)
-

- [Resolved Caveats—Cisco IOS Release 12.0\(28\)S6, page 1066](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(28\)S5, page 1081](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(28\)S4, page 1082](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(28\)S3, page 1101](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(28\)S2, page 1120](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(28\)S1, page 1147](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(28\)S, page 1193](#)
-

- [Resolved Caveats—Cisco IOS Release 12.0\(27\)S5, page 1252](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(27\)S4, page 1273](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(27\)S3, page 1293](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(27\)S2, page 1327](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(27\)S1, page 1354](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(27\)S, page 1363](#)
-

**Cross-Platform Release Notes for Cisco IOS Release 12.0S, Part 5:
Caveats for 12.0(26)S6 through 12.0(24)S**

- [Resolved Caveats—Cisco IOS Release 12.0\(26\)S6, page 1417](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(26\)S5, page 1424](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(26\)S4, page 1438](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(26\)S3, page 1446](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(26\)S2, page 1467](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(26\)S1, page 1502](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(26\)S, page 1534](#)
-

- [Resolved Caveats—Cisco IOS Release 12.0\(25\)S4, page 1630](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(25\)S3, page 1646](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(25\)S2, page 1652](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(25\)S1, page 1676](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(25\)S, page 1702](#)
-

- [Resolved Caveats—Cisco IOS Release 12.0\(24\)S6, page 1760](#)
- [Resolved Caveats—Cisco IOS Release 12.0\(24\)S5, page 1770](#)
- [Resolved Caveats—Cisco IOS Release 12.0\(24\)S4, page 1779](#)
- [Resolved Caveats—Cisco IOS Release 12.0\(24\)S3, page 1796](#)
- [Resolved Caveats—Cisco IOS Release 12.0\(24\)S2, page 1816](#)
- [Resolved Caveats—Cisco IOS Release 12.0\(24\)S1, page 1836](#)
- [Resolved Caveats—Cisco IOS Release 12.0\(24\)S, page 1853](#)

**Cross-Platform Release Notes for Cisco IOS Release 12.0S, Part 6:
Caveats for 12.0(23)S6 through 12.0(6)S**

- [Resolved Caveats—Cisco IOS Release 12.0\(23\)S6, page 1917](#)
- [Resolved Caveats—Cisco IOS Release 12.0\(23\)S5, page 1928](#)
- [Resolved Caveats—Cisco IOS Release 12.0\(23\)S4, page 1940](#)
- [Resolved Caveats—Cisco IOS Release 12.0\(23\)S3, page 1956](#)
- [Resolved Caveats—Cisco IOS Release 12.0\(23\)S2, page 1974](#)
- [Resolved Caveats—Cisco IOS Release 12.0\(23\)S1, page 1991](#)
- [Resolved Caveats—Cisco IOS Release 12.0\(23\)S, page 2003](#)

-
- [Resolved Caveats—Cisco IOS Release 12.0\(22\)S6, page 2049](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(22\)S5, page 2051](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(22\)S4, page 2060](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(22\)S3, page 2073](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(22\)S2, page 2085](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(22\)S1, page 2093](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(22\)S, page 2106](#)
-

- [Resolved Caveats—Cisco IOS Release 12.0\(21\)S8, page 2174](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(21\)S7, page 2175](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(21\)S6, page 2178](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(21\)S5, page 2184](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(21\)S4, page 2192](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(21\)S3, page 2196](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(21\)S2, page 2200](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(21\)S1, page 2210](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(21\)S, page 2214](#)
-

- [Resolved Caveats—Cisco IOS Release 12.0\(19\)S4, page 2234](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(19\)S3, page 2234](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(19\)S2, page 2235](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(19\)S1, page 2236](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(19\)S, page 2241](#)
-

- [Resolved Caveats—Cisco IOS Release 12.0\(18\)S7, page 2253](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(18\)S6, page 2254](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(18\)S5, page 2255](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(18\)S3, page 2255](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(18\)S2, page 2257](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(18\)S1, page 2258](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(18\)S, page 2261](#)
-

- [Resolved Caveats—Cisco IOS Release 12.0\(17\)S7, page 2270](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(17\)S6, page 2270](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(17\)S5, page 2271](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(17\)S4, page 2273](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(17\)S3, page 2275](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(17\)S2, page 2278](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(17\)S1, page 2280](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(17\)S, page 2288](#)
-

- [Resolved Caveats—Cisco IOS Release 12.0\(16\)S10, page 2300](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(16\)S9, page 2300](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(16\)S8, page 2301](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(16\)S3, page 2302](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(16\)S2, page 2304](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(16\)S1, page 2308](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(16\)S, page 2312](#)
-

- [Resolved Caveats—Cisco IOS Release 12.0\(15\)S7, page 2321](#)
- [Resolved Caveats—Cisco IOS Release 12.0\(15\)S6, page 2322](#)
- [Resolved Caveats—Cisco IOS Release 12.0\(15\)S3, page 2326](#)
- [Resolved Caveats—Cisco IOS Release 12.0\(15\)S1, page 2330](#)
- [Resolved Caveats—Cisco IOS Release 12.0\(15\)S, page 2332](#)

-
- [Resolved Caveats—Cisco IOS Release 12.0\(14\)S8, page 2339](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(14\)S7, page 2339](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(14\)S3, page 2339](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(14\)S1, page 2340](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(14\)S, page 2343](#)
-

- [Resolved Caveats—Cisco IOS Release 12.0\(13\)S8, page 2352](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(13\)S6, page 2353](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(13\)S, page 2353](#)
-

- [Resolved Caveats—Cisco IOS Release 12.0\(12\)S4, page 2361](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(12\)S3, page 2362](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(12\)S, page 2362](#)
-

- [Resolved Caveats—Cisco IOS Release 12.0\(11\)S6, page 2369](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(11\)S, page 2370](#)
-

- [Resolved Caveats—Cisco IOS Release 12.0\(10\)S8, page 2377](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(10\)S7, page 2378](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(10\)S, page 2378](#)
-

- [Resolved Caveats—Cisco IOS Release 12.0\(9\)S8, page 2383](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(9\)S, page 2383](#)
-

- [Resolved Caveats—Cisco IOS Release 12.0\(8\)S1, page 2387](#)
 - [Resolved Caveats—Cisco IOS Release 12.0\(8\)S, page 2387](#)
-

- [Resolved Caveats—Cisco IOS Release 12.0\(7\)S, page 2389](#)
-

- [Resolved Caveats—Cisco IOS Release 12.0\(6\)S, page 2390](#)
-

Resolved Caveats—Cisco IOS Release 12.0(33)S11

All the caveats listed in this section are resolved in Cisco IOS Release 12.0(33)S11. This section describes only severity 1, severity 2, and select severity 3 caveats

- CSCtw53776

Symptoms: A Cisco 12000 linecard crashes when NetFlow version 1 is configured on the router.

Conditions: The crash occurs if the “ip flow export x.x.x.x <port>” command is used instead of the “ip flow export destination x.x.x.x <port>” command.

Workaround: Configure NetFlow version 5 or version 9.

- CSCty77445

Symptoms: The SPA-2X1GE-V2 interface is in down/down status on RJ45 connection after moving the cable from RJ45 to SFP and back to RJ45 (SFP removed at the end).

Conditions: This symptom is observed when following these steps:

1. Make the interface up in RJ-45 mode (configure interface to RJ-45 mode with “media rj45” and you may also need to reboot the router without the SFP installed, if it is already in faulty condition).
2. Have the transceiver inserted into the corresponding SFP port and move the cable to the SFP.
3. Now, remove the transceiver and the cable together. Then move the cable to the RJ-45 port and that should trigger the problem. Port will not come up. Make sure that before you insert the cable into the RJ-45 port, the transceiver should be removed from the corresponding SFP port.

Workaround:

1. Use the SFP port.
2. Reload the router.

- CSCud28759

Symptoms: SPA crash is seen when invoking `spa_choc_dsx_cleanup_atlas_ci_config` with no data packed.

Conditions: This symptom is observed when the packed data size should be 1 and the status should be success.

Workaround: There is no workaround.

- CSCud28937

Symptoms: Two issues are observed:

1. Fasttag rewrite is not updated with new label after a route flap.
2. There are 2 load-shared paths and when one of the paths (say path2) goes down, the fasttag rewrite is not being set using path1. The **clear ip route *affected prefix*** command is needed to set the fasttag rewrite. Now if the path2 comes up, fasttag rewrite is not removed until you do a **clear ip route *affected prefix*** command.

Conditions: These symptoms are seen under the following conditions:

1. For the first issue, a Cisco 12000 series router connected to a non-Cisco device, which will send a new MPLS label to the Cisco 12000 series router after each session flap.
2. For the second issue, there should be two load-shared MPLS paths for a recursive destination prefix.

For both cases, the prefix should be a recursive prefix.

Workaround: Use the **clear ip route** *affected prefix* command for both issues.

- CSCue51713

Symptoms: Prefix changes its path from iBGP to eBGP.

Conditions: This symptom occurs when the same prefix is learned through two paths, iBGP and eBGP.

Workaround: Use the **clear ip route** *affected prefix* command.

Resolved Caveats—Cisco IOS Release 12.0(33)S10

All the caveats listed in this section are resolved in Cisco IOS Release 12.0(33)S10. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCed68723

Symptoms: Packets that are destined for an MPLS VPN may not reach their destination. The output of the **show ip cef vrf vrf-name detail** command may show the following tag information:

```
10.0.0.0/16, version 437, epoch 0, cached adjacency to POS4/0
0 packets, 0 bytes
  Flow: AS 0, mask 16
    tag information set, all rewrites inherited <-----
      local tag: assigned-when-resolved-later <-----
    via 10.1.1.1, 0, 0 dependencies, recursive
      next hop 10.2.2.2, POS4/0 via 10.1.1.1/32
      valid cached adjacency
```

Conditions: This symptom is observed on a Cisco router that is configured for MPLS VPN forwarding and CEF.

Workaround: Clear the affected route by entering the **clear ip route vrf vrf-name network mask** command.

- CSCsa49922

Symptoms: When an EIGRP internal route goes down, it may remain in the routing table although it is deleted from the EIGRP topology table.

Conditions: This symptom may occur when a router has an EIGRP internal route and an external route as the Successor and the Feasible Successor, respectively, for the same network and then the internal route goes down.

Workaround: Use either the internal route or the external route for the same network.

- CSCso88138

Symptoms: When there is a link flap or a reload, RSVP shows that the interface is down while actually the interface is up. Because of this, the tunnel may take a backup path even when the interface is up.

Conditions: Unknown at this time.

Workaround: Perform a **shut/no shut** on the interface.

- CSCsx08294

Symptoms: A Cisco 6500 running Cisco IOS Release 12.2(33)SXH may encounter a bus error due to OSPF processes.

Conditions: Occurs when the device is configured for OSPF Incremental SPF and Virtual Links.

Workaround: Do not use Incremental SPF.

- CSCtc90579

Symptoms: Router crashes due to memory corruption during MPLS TE auto backup tunnel deletion.

Conditions: Caused by topology changes triggering backup tunnel deletion and RSVP hello mechanism.

Workaround: Globally, disable RSVP hello and enable BFD hello:

```
Router(config)# no ip rsvp signalling hello
Router(config)# ip rsvp signalling hello bfd
Per MPLS TE enabled interface:
Router(config-if)# no ip rsvp signalling hello
Router(config-if)# ip rsvp signalling hello bfd
```

- CSCte80997

Symptoms: When a linecard is reloaded, the LFIB entries do not match the RP CEF entries. Reloading the linecard and clearing CEF and CEF adjacencies on the linecard do not clear the problem.

Conditions: eiBGP enabled so the routes are learned through an iBGP path and an eBGP path, multipath, CEF enabled.

Workaround: Add static default routes, one via the directly connected CE router with outgoing information as eBGP path and the other for the remote CE router with outgoing information as iBGP path.

- CSCtl82483

Symptoms: When there is a parent policy map on the main interface with “match vlan” and subinterfaces that have IPv6 traffic, after a shut and no shut of the main interface, the QoS for IPv6 traffic stops working.

Conditions: Using “match vlan” with the parent policy.

Workaround: Remove and reapply the policy map on the main interface. Also, if you enable the “debug eelc qos” command on the linecard, the problem goes away.

- CSCtn58005

Symptoms: The prefix-list does not filter local routes configured in the L1-L2 domain.

Conditions: The symptom is observed on a router running IPv6 ISIS L1-L2 domain and when L1 routes are redistributed into L2 routes.

Workaround: There is no workaround.

- CSCtq97113

Symptoms: High CPU utilization is observed on the linecard with the “CEF LC IPC Backg” process. It is followed by memory depletion in the RP, which results in the FIB being disabled.

Conditions: This symptom is observed when multipath load balancing is configured in the core network and these paths keep flapping.

Workaround: Stop the path flaps in the core network.

- CSCtr88610

Symptoms: Five Cisco 12000 series Internet routers have similar problems. Few free buffers are seen in the Tofab Q, and linecard fish_status stuck or ToFab Q stuck is seen. The E5 card crashes due to a ToFab FIA FIFO overflow.

SLOT 2:Aug 10 15:17:19.984 PRC: %FIA-3-FIFOERRS: To Fabric FIFO Error was detected. Cell FIFO Overflow, Data = 0x400, 0x2, 0x0, 0x0. SLOT 2:Aug 10 15:17:19.984 PRC: TFIA is halted. Waiting for RP to initiate recovery 044884: Aug 10 15:17:22.202 PRC: %FABRIC-3-ERR_HANDLE: Due to FIA HALT error, reconfigure FIA on slot 2

Conditions: On E5 cards with oversubscribed traffic to an egress linecard.

Workaround: Change the FIA FIFO threshold value to 33 from default value of 37.

Attach<Failed slot #>

```
test write 2 11400020 0x21
test write 2 11400022 0x21
test write 2 11400024 0x21
test write 2 11400026 0x21
test write 2 11400028 0x21
test write 2 1140002A 0x21
test write 2 1140002C 0x21
test write 2 1140002E 0x21
test write 2 11400030 0x21
test write 2 11400032 0x21
test write 2 11400034 0x21
test write 2 11400036 0x21
test write 2 11400038 0x21
test write 2 1140003A 0x21
test write 2 1140003C 0x21
test write 2 1140003E 0x21
```

- CSCts60315

Symptoms: Even after a TE tunnel goes down, CEF is stuck at “due for deletion”.

```
Router3# show ip cef x.x.x.0
x.x.x.0/29, version 24108960, epoch 0, cached adjacency x.x.x.x
0 packets, 0 bytes
    tag information from x.x.x.x/32, due for deletion, shared, all rewrites inherited
        local tag: tunnel head
        fast tag rewrite with Tu11111, point2point, tags imposed {360}
    Flow: AS 0, mask 29
    via x.x.x.x, 0 dependencies, recursive
        next hop x.x.x.x, GigabitEthernet2/1/0.z via x.x.x.x/32 (Default)
        valid cached adjacency
```

Conditions: Happens in customer environment only. Customer and TAC tried to recreate in the lab but failed.

Workaround: Issuing the clear ip route <prefix> command can help in some devices but not all.

- CSCtt03653

Symptoms: Packets that are destined to router local IP addresses (including routing protocol packets) are dropped when under observation.

Conditions: The source or destination IP address of the dropped packet is provisioned for Lawful Intercept.

Workaround: There is no workaround.

- CSCtt10671

Symptoms: At the customer site, it was seen that if the power manager is enabled, the 4-slot Cisco 12000 series chassis displays that the power is not sufficient to support three SIPs. This issue is not specific to the 4-slot chassis. Other chassis can also face this issue.

Conditions: This issue may occur if the chassis is running with a specific type of CSC/SFCs.

Workaround: There is no workaround.

- CSCtu19667

Symptoms: A router reports an lbl configuration sync failure similar to:

%REDUNDANCY-3-CONFIG_SYNC: Active and Standby lbl configuration out of sync

Conditions: This symptom is seen when “ip host” commands are modified.

Workaround: The errors are cosmetic and do not accurately reflect the state of the configuration sync.

- CSCtw53776

Symptoms: A Cisco 12000 linecard crashes when NetFlow version 1 is configured on the router.

Conditions: The crash occurs if the “ip flow export x.x.x.x <port>” command is used instead of the “ip flow export destination x.x.x.x <port>” command.

Workaround: Configure NetFlow version 5 or version 9.

- CSCtw61050

Symptoms: A ping with a large packet size fails.

Conditions: When there are more than seven buffer pools.

Workaround: Configure a carve-level default or reduce the set of MTUs so that none of the pools is reduced.

- CSCtx19461

Symptoms: If the BGP IPv6 table has a ::/X prefix present that is learned from another 6PE router, we see the following issues.

1. The 6PE router stops advertising the ::/0 prefix. Instead, it advertises the ::/X prefix that is present in the BGP table.
2. The 6PE router does not withdraw the ::/0 prefix.
3. Output from the “show bgp ipv6 unicast” command does not show prefix ::/0. Instead, it shows prefix ::/X.

Conditions: If the BGP IPv6 table has a ::/X prefix present that is learned from another 6PE router and you are advertising ::/0.

Workaround: There is no workaround.

- CSCtx36490

Symptoms: There is a stuck stale nexthop 0.0.0.0 for routes that are redistributed into EIGRP from BGP. This stale nexthop gets promoted to the top of the EIGRP topology table upon a route/router flap. This will result in a redistribution loop in the RIB.

Conditions: The redistribution loop in the RIB causes the route to be continuously installed in the RIB from BGP and EIGRP, resulting in a high number of CEF updates. This high number of CEF updates results in the RP running out of memory due to CSCtq97113.

Workaround: Clear out the stale nexthop 0.0.0.0 from the EIGRP topology table by issuing the “clear ip eigrp [vrf <vrf-name>] <AS-number> topology <prefix> <mask>” command.

In a PE-CE environment, if there is a peering between two PEs that are learning the prefix from the same CE site, the stale nexthop 0.0.0.0 could get promoted in the EIGRP topology table upon a route flap. This could, in turn, trigger the looping. To avoid this, you may remove any such redundant peering.

A detailed explanation of this workaround is provided in the enclosure “explanation of workaround”.

- CSCtx63661

Symptoms: When you configure “isis metric xxx” (xxx > 63) before “ip router isis ...”, the “isis metric xxx” command will not be synced to the standby RP.

Conditions:

1. xxx > 63
2. command sequence: “isis metric xxx” and then “ip router isis ...”

Workaround: Always configure “isis metric xxx” after “ip router isis ...”

- CSCuk31498

Symptoms: HSRP packets are sent with the IP TTL field set to 2 instead of 1.

Conditions: Unknown.

Workaround: There is no workaround.

Further Problem Description: This has no detrimental effect on the operation of HSRP. This will not cause HSRP packets to be forwarded since they are sent to a link-local multicast address.

Resolved Caveats—Cisco IOS Release 12.0(33)S9

All the caveats listed in this section are resolved in Cisco IOS Release 12.0(33)S9. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCsa43815

Symptoms: The following error message is seen:

```
%SCHED-7-WATCH: Attempt to lock uninitialized watched semaphore (address 0)
```

Conditions: This symptom is observed when memory is reserved using the **memory reserve critical 1000** configuration command, and a preemptive process is configured to run on the system.

Workaround: There is no known workaround yet.

- CSCsy73123

Symptoms: Connected route on port-channel subinterface is not removed when port-channel is down.

It can also happen whenever we have Superfund an IP address.

Conditions:

```
R1(config-if)# do show ip route 192.168.0.0
Routing entry for 192.168.0.0/23, supernet Known via "connected", distance 0, metric 0
 (connected, via interface) Routing Descriptor Blocks: * directly connected, via
 Ethernet0/0 Route metric is 0, traffic share count is 1

R1(config-if)# do show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D - EIGRP, EX
 - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 -
 OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E -
 BGP i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS
 inter area, * - candidate default, U - per-user static route o - ODR
Gateway of last resort is not set
C 192.168.0.0/23 is directly connected, Ethernet0/0 C 192.168.0.0/22 is directly
connected, Ethernet0/0 >> C 192.168.0.0/21 is directly connected, Ethernet0/0 >> C
192.168.0.0/20 is directly connected, Ethernet0/0 >> C 192.168.0.0/19 is directly
connected, Ethernet0/0 >>
```

In this case, we have superneted an IP address.

Workaround: If we have this scenario [superneted IP address], workaround is to use the **clear ip route *** command.

- CSCtc72553

Symptoms: An E5 linecard on a Cisco 12000 crashes.

Conditions: This symptom occurs with high traffic on OC48, E5, and possibly corrupt packets (MPLS packets without an MPLS label) received on the linecard.

The logs show the following:

```
Sep 30 01:41:01.958 PRC: %MBUS_SYS-3-NOBUFFER: Message from slot 1 in stream 1 dropped
Sep 30 01:41:02.062 PRC: %FIB-2-FIBDISABLE: Fatal error, slot 1: IPC Failure: timeout
Sep 30 01:41:02.062 PRC: %RP-4-RSTSLLOT: Resetting the card in the slot: 1,Event: CEF
failure
```

Workaround: There is no workaround.

Further Problem Description: The crash is seen on E5 OC48. Forwarding engine error interrupts are observed.

There is a basic configuration on the interface; a plain IPv4 configuration without MPLS.

- CSCtg22674

Symptoms: The router experiences high CPU for several minutes due to “MPLS TE LM” process.

Conditions: This symptom occurs when a router has many (perhaps as few as 100) MPLS TE tunnels that traverse over a link which experiences repeated flapping in a short duration.

Workaround: There is no workaround.

Further Problem Description: Use the **show process cpu** command to determine CPU utilization. If this problem exists, the MPLS TE LM process holds greater than 90-percent resources for 5 minutes or more.

```
CPU utilization for five seconds: 100%/0%; one minute: 100%; five minutes: 100% PID
Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process 216 867694836 18357673 47266
99.67% 99.09% 99.11% 0 MPLS TE LM
```

- CSCth87458

Symptoms: Memory leak detected in SSH process during internal testing. Authentication is required in order for a user to cause the memory leak.

Conditions: This was experienced during internal protocol robustness testing.

Workaround: Allow SSH connections only from trusted hosts.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.8/5.6:

<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:S/C:N/I:N/A:C/E:F/RL:OF/RC:C> CVE ID CVE-2011-2568

Has been assigned to document this issue. Additional information on Cisco’s security vulnerability policy can be found at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtj44454

Symptoms: The “SCP Read” process is at 99 percent, and the SCP session is stuck or not responding to commands.

Conditions: This symptom is seen when a secure copy session is started on a Cisco router running Cisco IOS Release 12.0(32)SY8 and later and the TCP session is closed—for whatever reason—on the client or server. After the TCP session is closed, the CPU spikes indefinitely.

Workaround: There is no workaround.

- CSCtj57910

Symptoms: A serial interface on a Cisco 12000 is Up/Down after a PRP switchover.

Conditions: This symptom can occur after a PRP switchover. Any Layer 2 encapsulation type (PPP, Frame Relay, and HDLC) is affected.

Workaround: Delete the interface (**no channel-group**) and recreate the interface (**channel-group**).

- CSCtk13378

Symptoms: High CPU utilization is experienced by the “CEF LC IPC Backg” process on the E5 card.

Conditions: When there are multiple loadbalancing paths and a “cef clear linecard” command is issued on the peer router or a shut/no shut is performed on one interface of this router, high CPU utilization occurs from the CEF process.

Workaround: There is no workaround.

- CSCtl04159

Symptoms: A BGP route map that is using a prefix list is not filtering outbound routes.

Conditions: A route map with a next hop and prefix list does not work.

Workaround: There is no workaround. You can use an access list if required.

- CSCto83346

Symptoms: After reloading a CE device connected via ATM to a Cisco 12000 series Internet router with an ATMoMPLS circuit, the CE device starts experiencing cell lost.

Conditions: PVP mode ATMoMPLS.

Workaround: Remove and re-add the xconnect configuration under the attachment circuit.

- CSCtq33005

Symptoms: When BFD goes down on a Cisco 12000 series router that is running Cisco IOS Release 12.0S, BGP may not tear the session down until the hold timer expires.

Conditions: This problem is seen on a subinterface that has been deleted and re-added.

Workaround: Create a new, unused subinterface and move the BFD session to the subinterface.

- CSCtq33480

Symptoms: New link bundling entries may stop forwarding traffic.

Conditions: This symptom is seen with CEF link bundling entries on Engine 3 line card. The entries appear corrupted.

Workaround: Reload line card.

- CSCtr89883

Symptoms: SPA IPC packets are getting corrupted due to MPLS packets received on the slow path.

Conditions: This symptom occurs only with IP options packets that are received from the MPLS core.

Workaround: Block the IP options packets.

- CSCtr98532

Symptoms: A Cisco 12000 series router that is running a Cisco IOS 12.0(32) SY6 image or later and that has an Engine 5 linecard and channelized SPAs might occasionally see a spurious SPA reload or linecard reload.

Conditions: This issue is seen only with channelized SPAs (1xCHOC3, 4xCT3, or 8xCHT1/E1) and when the Control Plane Policing feature is configured. If the CoPP configuration is configured to examine Layer 4 headers (for example, TCP, UDP, or ICMP), the issue might be seen. The issue is seen along with the L3VPN over IP feature.

Workaround: There is no workaround. The issue is very random in nature and is dependent on network configuration.

Resolved Caveats—Cisco IOS Release 12.0(33)S8

All the caveats listed in this section are resolved in Cisco IOS Release 12.0(33)S8. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCtg41086

Symptoms: A customer observed multiple errors on the E1 on the Cisco 7206 side, which caused the interface to bounce continuously. The customer created a test VC on the Cisco 12000 SPA and measured its clocking in comparison to the ethalon. The difference was with an accuracy of 10^{-3} , but it should be at least 10^{-6} . Further tests showed that the E1 on the Cisco 12000 takes clocking from the SPA card, although it should take clocking from the SIP linecard backplane.

Conditions: A Cisco 12000 with an SPA-1XCHSTM1/OC3 that is used for channelized E1.

Workaround: Turn the synchronization around in order for the other side to be the clocking source.

- CSCtg72961

Symptoms: A Cisco 12000 router may retain the old label for a VPNv4 route when the primary route has disappeared.

Conditions: This problem occurs when multiple routes for the same VPNv4 prefix exist and they all have the same next hop. You also need to have the **ip cef table loadinfo force** command configured on the router.

Workaround: Clear the affected route to recover from the problem.

- CSCth90331

Symptoms: Interface flaps on an ISE ATM LC running Cisco IOS Release 12.0(32) SY11 cause a leak in the encapsulation table (“show gsr ha encap-table slot3” for that LC, and the encapsulation table will fill up). When that happens, any interface that flaps or is bounced will not be able to pass outbound traffic.

To see the encapsulation table, issue the “show gsr ha encap-table slot#” command. If the table is full, every entry will be FFFFFFFF.

```
SNIP... 09BC9E60: FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF ..... 09BC9E70:
FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF ..... 09BC9E80: FFFFFFFF FFFFFFFF
FFFFFFFF FFFFFFFF ..... 09BC9E90: FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
..... 09BC9EA0: FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF .....
09BC9EB0: FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF ..... 09BC9EC0: FFFFFFFF
FFFFFFFF FFFFFFFF FFFFFFFF ..... 09BC9ED0: FFFFFFFF FFFFFFFF FFFFFFFF
FFFFFFFF ..... 09BC9EE0: FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
..... 09BC9EF0: FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF .....
```

Conditions: This symptom is observed on an ISE ATM LC that is running Cisco IOS Release 12.0(32)SY11.

Workaround: Stop any excessive interface flapping to prevent the encapsulation table from filling up. If it is full, a microcode reload of the affected LC will clear the table.

- CSCth95192

Symptoms: On a Cisco router loaded with Cisco IOS Release 12.0(33)S6, when LSP changes, the CEF table may become stuck with old label information.

Conditions: This symptom occurs when there are two outgoing links to the BGP next hop for the prefix received via BGP.

The following is a snapshot of how the CEF table will be during the time of the issue:

```
R1# show ip cef 10.150.150.150 detail
```

```
10.150.150.150/32, version 26, epoch 0, cached adjacency 10.1.15.5 0 packets, 0 bytes
tag information from 10.100.100.0/30, shared, all rewrites owned local tag: 33 fast
tag rewrite with Et0/0.12, 10.1.1.1, tags imposed {16} via 10.100.100.2, 0
dependencies, recursive next hop 10.1.15.5, Ethernet0/0.15 via 10.100.100.0/30
(Default) valid cached adjacency tag rewrite with Et0/0.15, 10.1.15.5, tags imposed
{502}
```

Workaround: Issue the “clear ip route” command.

- CSCti08185

Symptoms: WRED Min and Max threshold values appear as “0” in “show policy-map interface” output on an RP.

Conditions:

1. There are many multilink interfaces on a Cisco 12000 node bearing policies that have class maps sharing the same WRED min/max threshold configuration.
2. The multilink interfaces must have multiple members (the more members, the more the probability to hit the issue).
3. There must be a series of member addition/deletion events at the same time, such as during a reload.
4. The order in which the interfaces (the members of these multilink interfaces) come up also plays a role in hitting the issue.

Workaround:

1. Remove and re-apply the service policy (this will surely resolve the issue; however this is more of a recovery procedure).
2. Perform a shut/no shut on the interface (again, a recovery procedure; traffic impacting as well).
3. Before the upgrade, you can identify the policy (with the WRED configuration) that is attached to more than one multilink interface (with more than one member link). Remove that policy from the interface and apply it back after the upgrade after all member links of the interface have come up.

- CSCti24849

Symptoms: Available interface bandwidth goes down for the Jag48/FB type of interfaces even when there is no policy on the main or subinterfaces.

Conditions:

1. The Jag48/FB card which will fall in to types which share same conga port per main interface and its subinterfaces.

2. Apply BT QoS (parent with dummy child) on the main interface.
3. Apply flat policy (with priority + police) on the subinterface.
4. Remove flat policy from the subinterface.

Workaround: Apply, again, policies to the main and subinterface. Remove the BT QoS from the main interface first and then remove the policy from the subinterface.

- CSCti55312

Symptoms: When multilink interfaces (connected to CE device) are flapped on a Cisco 12000, the Cisco 12000 hardware does not set the HW adjacency correctly. It happens because LDP assigns imp-null instead of a real local label after multilink comes up.

Conditions: Static route pointing to multilink interfaces.

Workaround: Force LDP to assign a real local label instead of an imp-null after multilink comes up with shut/no shut on affected multilink interface.

Further Problem Description: Hardware CEF adjacency is NULL at ingress LC, for few static route prefixes going through multilink interfaces. It seems to occur when LDP does not assign a real label for a prefix, but this is a coincidence, not the root cause of the HW IP entry being NULL.

- CSCti88244

Symptoms: Frequent flapping of Serial interfaces (E1) that are part of an MLPPP bundle may cause a PLIM Cause 0 reset. After the PLIM RESET recovery, some interfaces remain in the Up/Down state.

Conditions: Frequent flapping of Serial links that are part of an MLPPP bundle in Cisco IOS Release 12.0(33)S6.

Workaround: A PLIM RESET due to cause 1 is a recovery mechanism to reset the PLIM provisioning ASIC from its stuck condition. For interfaces that are in the Up/Down state after the PLIM recovery, a shut/no shut on Serial interfaces has to be done to recover the interfaces to operational status.

Resolved Caveats—Cisco IOS Release 12.0(33)S7

All the caveats listed in this section are resolved in Cisco IOS Release 12.0(33)S7. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCsv73754

Symptoms: A router crashes during VRF configuration. A traceback decode points to a function `bgp_vpn_impq_add_vrfs_cfg_changes`.

Conditions: The symptom is observed while unconfiguring VRFs. It is most likely to be seen when 100 VRFs or more are unconfigured.

Workaround: There is no workaround.

- CSCsw63003

Symptoms: Memory increase occurs in “BGP Router” process due to BGP path attributes. Memory used by this process increase every day and so do the BGP path attributes while the number of routes is not increasing.

Conditions: This occurs on a provider edge (PE) router running Cisco IOS Release 12.2(31)SB, 12.2(33)SB, 12.2(33)SRB, 12.2(33)SRC, 12.2(33)SRD, 12.4, and 12.4T. Problem is seen with continuous churn in the network such that BGP never manages to converge and when the paths churning are not reusing existing path attributes. That will cause those paths to allocate new paths attributes.

Workaround: Reload the router if low memory conditions are reached or identify the root cause of the churn and attempt to fix that is possible.

- CSCsy58115

Symptoms: In a router that is running BGP, the BGP process may hold increased amounts of memory over time without freeing any memory. This symptom may also be seen in the output of the **show proc mem sort** command and in the output of the **show ip bgp sum** or **show ip bgp vpnv4 all sum** commands and by looking at the number of BGP attributes, which may be increasing over time in relation to the BGP prefixes and paths, which may remain roughly the same.

Conditions: Some BGP neighbors are not in an established state and are not exchanging prefixes.

Workaround: Remove the configuration lines related to the inactive neighbors (neighbors in the Idle or Active states).

- CSCsy83266

Symptoms: A router experiences CPU hog or crashes when doing snmpwalk.

Conditions: This symptom is observed when interfaces are attached with a large-scale police configuration (for example, a two-level policy map, 200 (parent classes) x 15 (child classes) = 3000 policers).

Workaround: There is no workaround for walking the table. To get a specific entry, use snmpget.

- CSCsz12469

Symptoms: It was observed on a Cisco 12816 router that was running Cisco IOS Release 12.0(32)S6r that some linecard would not fully load to STRTIOS. Some slot would not completely boot a linecard, which would be stuck in WAITTRY.

Conditions: The following can be observed in the log when this symptom occurs on slot 11:

```
%MBUS_SYS-3-NOBUFFER: Message from slot 11 in stream 1 dropped %PRP-3-CHP_DESCQ_FULL:
Chopper desc queue 11 full - enq 3383072 deq 3382050 blog 1022 -Traceback= 2044B0
2045B8 534840 535218 5353A4 351284 351350 5F6BE8 60AD34 5FA7D0 5FB24C 2EDFBC
```

Workaround: If route-processor redundancy exists, an RP forced switchover can reset the Chopper queue and clear the issue. If there is not a redundant RP, an RP reload will also clear the Chopper queue.

- CSCtb03758

Symptoms: Traffic drops are observed on serial interfaces that are configured with L2VPNs.

Conditions: This symptom is observed when a microcode reload is performed on the linecard.

Workaround: Perform a shut/no shut on the serial interface on PE1.

- CSCtb25496

Symptoms: New Excellight SFP part was being tested as part of Manufacturing change process MCN-22773. A few SFP parts failed security check in Cisco IOS software because the data read from the EEPROM in SFP was FF in some locations. This was further root-caused to the fact that there is some timing violation on I2C bus to SFP for reading the EPROM data. The I2C interface is register-mapped on the FPGA, and the software toggles two bits in the register to control the I2C protocol. Read is the only operation performed on the bus. During a read operation, after every data byte is read from the I2C slave (SFP), the bus floats for I2C master (FPGA) to return ACK to slave.

This is the ninth clock cycle of SCL. SDA driven low during SCL's rising edge is detected as ACK. But here, the SDA is driven low during falling edge of SCL. That means, SDA's falling edge coincides with SCL's falling edge. This may sometimes be detected as a START condition by the slave (the START condition is a LOW on SCL during falling edge of SDA). The SFP state machine is disturbed with this, and it probably goes into START mode. So, the SFP does not drive any data onto the bus, whereas the master reads FF on the bus because the default state of SDA is HIGH.

Conditions: An SFP OIR.

Workaround: There is no workaround.

- CSCtb73450

Symptoms: Start-Control-Connection-Request (SCCRQ) packets may cause a tunnel to reset after digest failure.

Conditions: This symptom occurs when the SCCRQ packets are sent with a wrong hash.

Workaround: There is no workaround.

- CSCtc14824

Symptoms: Interface flapping in a link bundling may cause the linecards to crash.

Conditions: When an Engine 5 linecard and a Gigabit SPA are configured as part of a LB member and when bidirectional multicast traffic is sent through the LB interface that goes down, the linecard may crash.

Workaround: Perform one of the following two options:

Option 1: Where possible, consider building a port-channel from the same slot. For example, if your present configuration has the following:

```
!
interface GigabitEthernet0/1/1
  channel-group 1
!
interface GigabitEthernet1/0/0
  channel-group 1
!
```

Then consider the following, if feasible:

```
!
interface GigabitEthernet0/1/1
  channel-group 1
!
interface GigabitEthernet0/2/0 <=== (channel-gr 1 from Gi 1/0/0 to Gi 0/2/0)
  channel-group 1
!
```

Option 2: This crash is seen when there is user intervention that leads to physical interaction with the module/interface hardware, when traffic is actively flowing. Consider shutting the interfaces down before touching the hardware/interfaces.

- CSCtc45384

Symptoms: IPv6 packets stop matching Class in the service policy when a shut/no shut of the interface is performed.

Conditions: This symptom is observed when a shut/no shut is performed on the interface.

Workaround: Remove and reapply the service policy.

- CSCtc61836

Symptoms: MLPPP sequence numbers received by the remote end have missing sequences and/or interrupted multicast traffic with the MLPPP interface as the outgoing link.

Conditions: This symptom is observed under the following conditions:

- The MLPPP interface is configured with multicast. - Physical errors exist in the line that trigger autoDNR.

Workaround:

- Disable multicast on the MLPPP link.

Recovery:

- Shut/unshut a member link.
- Clear the mroute table using the clear up mroute vrf <vrf name> * command.

- CSCtc79299

Symptoms: Sending IPv6 traffic with hop-by-hop headers causes the RP CPU utilization to spike up to 40 percent.

Conditions: This symptom is observed in IPv6 traffic with hop-by-hop headers.

Workaround: There is no workaround.

- CSCtd18657

Symptoms: The following message appears:

```
%TFIB-7-SCANSABORTED: TFIB scan not completing. MAC string updated.
```

Conditions: This symptom is observed on a Cisco 12000 series router. The router has a great number of prefixes for which the output interface is an MPLS Traffic Engineering tunnel.

Workaround: There is no workaround.

- CSCtd29170

Symptoms: A Cisco router may unexpectedly reload due to a bus error when removing a route map.

Conditions: The route map must have more than one sequence number, and under one of the route-map sequence numbers there must be a “match ipv6 address <acl>” entry in which the ACL does not exist.

Workaround: Remove the “match ipv6 address” statement from the route map before removing the route map itself.

- CSCtd46318

Symptoms: Multiple tracebacks are seen on the standby route processor.

Conditions: This symptom is observed during router bootup.

Workaround: Reload the router again.

- CSCtd46847

Symptoms: In an APS setup involving CHOC12 linecards, the APS switches over from the Working line to the Protect line for different reasons like LAIS, LOF/LOS, and SF and SD conditions.

Conditions: This symptom is observed on a Cisco 12000 series router that is running Cisco IOS Release 12.0(32)S11q. The issue is applicable only to CHOC12 linecards.

Workaround: There is no workaround.

Further Problem Description: The alarms that are responsible for APS switchover are spurious. The alarm counters on the SONET controller could be huge in successive **show controller** captures.

- CSCtd54941

Symptoms: Increased PLIM resets on the CHOC12 Line cards might be seen on some nodes.

Conditions: This symptom is observed in a normal production environment when running images post 12.0(32)S9, 12.0(32)SY05, 12.0(33)S.

Workaround: There is no workaround

- CSCtd62350

Symptoms: Exporting with the VRF aware feature is not working, except if we export to a device that is reachable via the global routing table.

```
ip flow-export version 9
ip flow-export destination 10.116.244.61 63636 vrf gestion ip flow- aggregation cache
protocol-port export destination 10.116.244.61 63636 vrf gestion
```

- Sourced from global loopback interface, same
- Sourced from same VRF interface where to export, same
- Changed sample interval to minimum, same

The output looks fine. You can see the packets being sent from the Cisco 12000, and there are no IPC drops; however the sniffer is not showing anything.

Conditions: This symptom is observed on a Cisco 12000 that is using NetFlow with VRF support.

Workaround: Use the global routing table.

- CSCtd75033

Symptoms: Cisco IOS Software is affected by NTP mode 7 denial-of-service vulnerability. Note: The fix for this vulnerability has a behavior change affect on Cisco IOS Operations for Mode 7 packets. See the section Further Problem Description of this release note enclosure.

Conditions: Cisco IOS Software with support for Network Time Protocol (NTP) contains a vulnerability processing specific NTP Control Mode 7 packets. This results in increased CPU on the device and increased traffic on the network segments.

This is the same as the vulnerability which is described in <http://www.kb.cert.org/vuls/id/568372>.

Cisco has release a public facing vulnerability alert at the following link:

<http://tools.cisco.com/security/center/viewAlert.x?alertId=19540>

Cisco IOS Software that has support for NTPv4 is NOT affected. NTPv4 was introduced into Cisco IOS Software: 12.4(15)XZ, 12.4(20)MR, 12.4(20)T, 12.4(20)YA, 12.4(22)GC1, 12.4(22)MD, 12.4(22)YB, 12.4(22)YD, 12.4(22)YE, and 15.0(1)M.

All other versions of Cisco IOS and Cisco IOS XE Software are affected.

To see if a device is configured with NTP, log into the device and issue the CLI command **show running-config | include ntp**. If the output returns either of the following commands listed then the device is vulnerable:

```
ntp master <any following commands>
ntp peer <any following commands>
ntp server <any following commands>
ntp broadcast client ntp multicast client
```

The following example identifies a Cisco device that is configured with NTP:

```
Router# show running-config | include ntp ntp peer 192.168.0.12
```

The following example identifies a Cisco device that is not configured with NTP:

```
Router# show running-config | include ntp
```

To determine the Cisco IOS Software release that is running on a Cisco product, administrators can log in to the device and issue the `show version` command to display the system banner. The system banner confirms that the device is running Cisco IOS Software by displaying text similar to “Cisco Internetwork Operating System Software” or “Cisco IOS Software.” The image name displays in parentheses, followed by “Version” and the Cisco IOS Software release name. Other Cisco devices do not have the `show version` command or may provide different output.

The following example identifies a Cisco product that is running Cisco IOS Software Release 12.3(26) with an installed image name of C2500-IS-L:

```
Router # show version
```

```
Cisco Internetwork Operating System Software IOS (tm) 2500 Software (C2500-IS-L),
Version 12.3(26), RELEASE SOFTWARE (fc2) Technical Support:
http://www.cisco.com/techsupport Copyright ) 1986-2008 by cisco Systems, Inc.
Compiled Mon 17-Mar-08 14:39 by abcde
<output truncated>
```

The following example shows a product that is running Cisco IOS Software release 12.4(20)T with an image name of C1841-ADVENTERPRISEK9-M:

```
Router# show version
```

```
Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version 12.4(20)T,
RELEASE SOFTWARE (fc3) Technical Support: http://www.cisco.com/techsupport Copyright )
1986-2008 by Cisco Systems, Inc. Compiled Thu 10-Jul-08 20:25 by prod_rel_team
<output truncated>
```

Additional information about Cisco IOS Software release naming conventions is available in “White Paper: Cisco IOS and NX-OS Software Reference Guide” at the following link:

<http://www.cisco.com/web/about/security/intelligence/ios-ref.html>

Workaround: There are no workarounds other than disabling NTP on the device. The following mitigations have been identified for this vulnerability; only packets destined for any configured IP address on the device can exploit this vulnerability. Transit traffic will not exploit this vulnerability.

Note: NTP peer authentication is not a workaround and is still a vulnerable configuration.

* NTP Access Group

Warning: Because the feature in this vulnerability utilizes UDP as a transport, it is possible to spoof the sender’s IP address, which may defeat access control lists (ACLs) that permit communication to these ports from trusted IP addresses. Unicast Reverse Path Forwarding (Unicast RPF) should be considered to be used in conjunction to offer a better mitigation solution.

! Configure trusted peers for allowed access.

```
access-list 1 permit 171.70.173.55
```

! Apply ACE to the NTP configuration.

```
ntp access-group peer 1
```

For additional information on NTP access control groups, consult the document titled “Performing Basic System Management” at the following link:

http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_basic_sys_manage.html#wp1034942

* Infrastructure Access Control Lists

Warning: Because the feature in this vulnerability utilizes UDP as a transport, it is possible to spoof the sender's IP address, which may defeat ACLs that permit communication to these ports from trusted IP addresses. Unicast RPF should be considered to be used in conjunction to offer a better mitigation solution.

Although it is often difficult to block traffic that transits a network, it is possible to identify traffic that should never be allowed to target infrastructure devices and block that traffic at the border of networks.

Infrastructure ACLs (iACLs) are a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for this specific vulnerability. The iACL example below should be included as part of the deployed infrastructure access-list, which will help protect all devices with IP addresses in the infrastructure IP address range:

! Feature: Network Time Protocol (NTP)

```
access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
INFRASTRUCTURE_ADDRESSES WILDCARD eq 123
```

Note: If the router is acting as a NTP broadcast client via the interface command "ntp broadcast client" then broadcast and directed broadcasts must be filtered as well. The following example covers an infrastructure address space of 192.168.0.X.

```
access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD host 192.168.0.255
eq ntp access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD host
255.255.255.255 eq ntp
```

Note: If the router is acting as a NTP multicast client via the interface command "ntp multicast client" then multicast IP packets to the multicast group must be filtered as well. The following example covers a NTP multicast group of 239.0.0.1 (default is 224.0.1.1).

```
access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD host 239.0.0.1 eq ntp
```

! Deny NTP traffic from all other sources destined to infrastructure addresses.

```
access-list 150 deny udp any INFRASTRUCTURE_ADDRESSES WILDCARD eq 123
```

! Permit/deny all other Layer 3 and Layer 4 traffic in accordance with existing security policies and configurations. Permit all other traffic to transit the device.

```
access-list 150 permit ip any any
```

! Apply access-list to all interfaces (only one example shown).

```
interface fastEthernet 2/0 ip access-group 150 in
```

The white paper entitled "Protecting Your Core: Infrastructure Protection Access Control Lists" presents guidelines and recommended deployment techniques for infrastructure protection access lists and is available at the following link:

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml

* Control Plane Policing

Provided under Control Plane Policing there are two examples. The first aims at preventing the injection of malicious traffic from untrusted sources, whilst the second looks at rate limiting NTP traffic to the box.

- Filtering untrusted sources to the device.

Warning: Because the feature in this vulnerability utilizes UDP as a transport, it is possible to spoof the sender's IP address, which may defeat ACLs that permit communication to these ports from trusted IP addresses. Unicast RPF should be considered to be used in conjunction to offer a better mitigation solution.

Control Plane Policing (CoPP) can be used to block untrusted UDP traffic to the device. Cisco IOS software releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP can be configured on a device to help protect the management and control planes and minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic that is sent to infrastructure devices in accordance with existing security policies and configurations. The CoPP example below should be included as part of the deployed CoPP, which will help protect all devices with IP addresses in the infrastructure IP address range.

! Feature: Network Time Protocol (NTP).

```
access-list 150 deny udp TRUSTED_SOURCE_ADDRESSES WILDCARD any eq 123
```

! Deny NTP traffic from all other sources destined to the device control plane.

```
access-list 150 permit udp any any eq 123
```

! Permit (Police or Drop)/Deny (Allow) all other Layer3 and Layer4 traffic in accordance with existing security policies and configurations for traffic that is authorized to be sent to infrastructure devices. Create a Class-Map for traffic to be policed by the CoPP feature.

```
class-map match-all drop-udp-class match access-group 150
```

! Create a Policy-Map that will be applied to the Control-Plane of the device.

```
policy-map drop-udp-traffic class drop-udp-class drop
```

! Apply the Policy-Map to the Control-Plane of the device.

```
control-plane service-policy input drop-udp-traffic
```

In the above CoPP example, the access control list entries (ACEs) that match the potential exploit packets with the “permit” action result in these packets being discarded by the policy-map “drop” function, while packets that match the “deny” action (not shown) are not affected by the policy-map drop function.

- Rate Limiting the traffic to the device The CoPP example below could be included as part of the deployed CoPP, which will help protect targeted devices from processing large amounts of NTP traffic.

Warning: If the rate-limits are exceeded valid NTP traffic may also be dropped.

! Feature: Network Time Protocol (NTP).

```
access-list 150 permit udp any any eq 123
```

! Create a Class-Map for traffic to be policed by the CoPP feature.

```
class-map match-all rate-udp-class match access-group 150
```

! Create a Policy-Map that will be applied to the Control-Plane of the device. NOTE: See section “4. Tuning the CoPP Policy” of

http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html#5 for more information on choosing the most appropriate traffic rates.

```
policy-map rate-udp-traffic class rate-udp-class police 10000 1500 1500 conform-action transmit  
exceed-action drop violate-action drop
```

! Apply the Policy-Map to the Control-Plane of the device.

```
control-plane service-policy input drop-udp-traffic
```

Additional information on the configuration and use of the CoPP feature can be found in the documents, “Control Plane Policing Implementation Best Practices” and “Cisco IOS Software Releases 12.2 S - Control Plane Policing” at the following links:

http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrtlmt.html

Further Problem Description: Cisco IOS Software releases that have the fix for this Cisco bug ID, have a behavior change for mode 7 private mode packets.

Cisco IOS Software release with the fix for this Cisco bug ID, will not process NTP mode 7 packets, and will display a message “NTP: Receive: dropping message: Received NTP private mode packet. 7” if debugs for NTP are enabled.

To have Cisco IOS Software process mode 7 packets, the CLI command **ntp allow mode private** should be configured. This is disabled by default.

- CSCtd90953

Symptoms: A ping delay is observed on E5 interfaces.

Conditions: This symptom is observed after a CSC switchover is performed.

Workaround: Reload the linecard.

- CSCtd93825

Symptoms: When the E4+ linecard is inserted into a blank slot of a Cisco 12000 series router, the MAC addresses of that linecard becomes 0000.0000.0000.

Conditions: This symptom does not occur if the system boots with the linecard; this symptom occurs only when the E4+ linecard is inserted into a blank slot after booting is complete.

Workaround: Reload the system.

- CSCte45025

Symptoms: The main Gigabit interface flaps.

Conditions: This symptom occurs when a Gigabit subinterface with an IPv6 address is deleted.

Workaround: There is no workaround.

- CSCte83282

Symptoms: Submillisecond drops of ATM cells going over AToM pseudo-wire MPLS are observed.

Conditions: This symptom occurs whenever the TE tunnel used by the pseudo-wire is reoptimized.

Workaround: If possible, avoid the trigger for reoptimization (such as auto-bw or loose path).

- CSCte83622

Symptoms: High CPU utilization is seen on Cisco IOS Release 12.0(33)S5 code due to “RIP Send” and “BGP Scanner.”

Conditions: RIP in Cisco IOS Release 12.0(33)S does not have a separate database about the routes. When RIP has to send update packets, it will scan the whole routing table, validate each prefix and create the update packets and send out. Above event will have to happen every 15 seconds as per the timers configuration.

With a network where there are 150,000 routes learned by BGP, it is quite possible the routing table scan during update generation can be CPU intensive.

We will see the problem of continuous rip updates and high CPU until an RIP Send process.

Please note that a Supernet prefix needs to be installed in the RIB, and RIP has to include them in its updates. If it is originated by static or other routing protocols, we will see the symptom if they are redistributed into RIP.

Workaround: Filter the supernet redistribution. See the following example:

```
access-list 20 deny X.X.X.X 0.0.3.255 >>> Need to add all the prefixes to this ACL.
access-list 20 permit any
!
route-map supernet
match ip address 20
!
router rip
address-family ipv4 vrf <vrf>
redistribute <protocol> route-map supernet metric <metric>
```

- CSCtf05860

Symptoms: A connected route in VRF does not show up in the BGP VRF table, even though the redistribute connected is present.

There were no specific events before the issue. The customer configured a *new* subinterface, put it in the VRF, and configured a prefix on it. They discovered that it was not present in the BGP VRF table.

Note that when the show ip bgp vpnv4 RD x:x <prefix> <mask> command is entered, that prefix shows up as imported in a VRF that has nothing to do with the original one, not even importing its route-targets.

Conditions: This symptom is observed on a Cisco 12000 series router. VRF configuration/reconfiguration was done.

Workaround: Perform a standby switchover.

- CSCtf08444

Symptoms: A Cisco 12010/PRP-2 that is running Cisco IOS Release 12.0(33)S3/S4 linecards crashes.

Conditions: This symptom is observed after “ip flow monitor” is applied to the interface.

Workaround: There is no workaround.

- CSCtf14397

Symptoms: When “bgp send-label” is used along with LDP along the path, the label information for a prefix learned via iBGP multipath is not updated in the FIB and LFIB table after the route flaps. This symptom happens intermittently.

Conditions: This symptom is observed when “bgp send-label” is used along with LDP along the path.

Workaround: Enter the clear ip route x.x.x.x command for the prefix in question.

- CSCtf65144

Symptoms: The local LDP binding is not updated with the imp-null label for a summary route after the summary address is added in OSPF.

Conditions: This symptom occurs when the summary prefix is already learned from an OSPF neighbor, and the local label for the summary prefix is assigned.

Workaround: Enter the clear ip route <summary-prefix> command.

- CSCtg52659

Symptoms: An active RP crashes in the APS - PGP Message HA Sync to Standby event.

Conditions:

1. The standby RP does not respond to IPC communication during its reload.
2. APS is configured.
3. RPR+ or SSO mode is configured.

Workaround: It is a rare timing issue in the base code. To reduce the probability of occurrence, one can increase the APS PGP hello/hold timers before a scheduled standby RP reload.

Resolved Caveats—Cisco IOS Release 12.0(33)S6

All the caveats listed in this section are resolved in Cisco IOS Release 12.0(33)S6. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCeb53438

Symptoms: When you manually set the value of the *ring-limit* argument in the **tx-ring-limit ring-limit** interface configuration command, the value is lost when you reload the router, even though the value is properly saved in the running configuration and in the startup configuration.

Conditions: This symptom is observed only when you manually set the value of the *ring-limit* argument for an 8-port multichannel T1/E1 PRI port adapter (PA-MC-8TE1+) and you reload the router.

Workaround: There is no workaround.

- CSCef02332

Symptoms: A Cisco 7200 series with high-speed serial interfaces such as HSSI interfaces or PA-2T3+ interfaces may reload unexpectedly.

Conditions: This symptom is observed after you have performed an OIR of the HSSI or PA-2T3+ port adapter while traffic was being processed.

Workaround: Stop the traffic while you perform the OIR or shut down the port adapter before you perform the OIR.

- CSCej00344

Symptoms: A router may reload unexpectedly when opening a terminal session.

Conditions: This can be seen on any platform. It can be seen when starting any terminal session from the router, including a mistyped command which the router by default will try to resolve as an address to telnet to.

Workaround: There is no workaround.

- CSCin11687

Symptoms: When primary and backup Non-Facility Associated Signaling (NFAS) controllers are configured on a PA-MCX port adapter, upon shutting down the primary controller, Layer 1 of both the backup and primary controllers becomes deactivated. The backup D channel does not take over.

Conditions: This symptom is observed on a Cisco 7200 series router that is running Cisco IOS Release 12.2(10.5)T.

Workaround: Enter the **no shutdown** interface configuration command, followed by the **shutdown** interface configuration command, followed again by the **no shutdown** interface configuration command on the serial interface of the primary controller.

Alternate Workaround: Configure primary and backup NFAS members on a PA-VXC port adapter and do not configure NFAS members on the PA-MCX port adapter.

- CSCsa58277

Symptoms: All packets toward a specific adjacency get black-holed. The output of show controllers rewrites command on the output E4 linecard indicates that a bad destination MAC is being used for the rewrite.

For example:

```
LC-Slot1# show controllers rewrites | b 192.168.2.1
Port-channel2 192.168.2.1 0xE0307CC GigabitEthernet1/2/1 00E0812B28E5000E393CF5010800
----- incorrect
```

Conditions: This symptom is observed on a Cisco 12000 series Internet router that is running Cisco IOS Release 12.0(30)S and that is connected via a link-bundling interface (E4 LC) through a switch to numerous BGP peers, after one of the peers went down because of a long maintenance window.

Workaround: Clearing the adjacencies does not help; the only workaround possible is to remove link-bundling.

- CSCsd95545

Symptoms: Long unconfiguration times are seen for very large QoS configurations (in excess of 40,000 policy maps).

Conditions: This symptom is observed in Cisco IOS Releases 12.2SB and 12.4T.

Workaround: There is no workaround.

- CSCsi61988

Symptoms: On a Cisco 12000 series router that is running Cisco IOS Release 12.0(31)S6, a Malloc failure is seen on “L3 Engine: 6 - Backbone 2P OC192/ 8P OC48 (20 Gbps)”:

```
SLOT 10:Mar 29 12:41:01: %SYS-2-MALLOCFAIL: Memory allocation of 65556 bytes failed
from 0x400DD7C8, alignment 32 Pool: Processor Free: 152456 Cause: Memory fragmentation
Alternate Pool: None Free: 0 Cause: No Alternate pool
```

Conditions: Multicast should be enabled because the memory leak happens from “MDFS LC Process.”

Workaround: Reload the linecard.

- CSCsk35688

Symptoms: Aggregate routes are not processed if all aggregated child routes are deleted prematurely.

Conditions: The symptom is observed when all aggregated child routes are marked for deletion and the periodic function which processes the routes to be deleted deletes the route before the aggregate processing function gets a chance to process them and the aggregate route to which they belong.

Workaround: Configuring “bgp aggregate-timer” to 0 or the lowest value would considerably reduce the chances of hitting this problem. In case this problem does occur, in order to delete the stale aggregate route, configure a temporary local BGP route (say, redistribute a static route or network a loopback) with its address being a subnet of the stale aggregate address and then remove the aggregate address and the added route. This should delete the route from table and send withdraws to the other routes also.

Further Problem Description: The periodic function is by default called at 60-second intervals. The aggregate processing is normally done based on the CPU load. If there is no CPU load, then the aggregate processing function would be triggered within one second. As the CPU load increases,

this function call will be triggered at higher intervals and if the CPU load is very high it could go as high as the maximum aggregate timer value configured via command. By default this maximum value is 30 seconds and is configurable with a range of 6 to 60 seconds and in some trains 0. So, if default values are configured, then as the CPU load increases, the chances of hitting this defect is higher.

- CSCsq73479

Symptoms: A Cisco 7200 series router that is loaded with Cisco IOS Release 12.0(33)S1 crashes while sending traffic through a PA-POS-1OC3 interface.

Conditions: A traffic-shaping service policy is attached to the PA-POS-1OC3 interface.

Workaround: There is no workaround.

- CSCsr24425

Symptoms: There were two symptoms reported for this problem:

1. Continuous increment in the mdfs reload count for some linecards.
2. Clearing of all entries in the global multicast routing table.

This leads to the loss of PIM neighborship with some peer routers.

Conditions: This problem is seen when the number of swidb or hwidb interfaces is at least 1638 in number, and the traffic is active.

Workaround: Configure additional interfaces, like a loopback interface, to resolve the reported issue. But there could still be wrong statistic updates and wrong show interface output.

- CSCsr97753

Symptoms: Pinging an interface fails.

Conditions: Occurs when unconfiguring xconnect on the interface.

Workaround: Perform a **shut/no shut** on the interface.

- CSCsu06930

Symptoms: A traceback and an error message are observed while provisioning/unprovisioning MFR on a CT3 SPA.

Conditions: A script is used that performs a sequence of events. MFR is configured for mVRF.

Workaround: There is no workaround.

- CSCsu24425

Symptoms: Standby RP can crash upon boot up.

Conditions: The symptom is observed under the following conditions:

1. "clock timezone . . ." is configured.
2. config-register = 0x2142.
3. The router is running Cisco IOS Release 12.0S based code.

Workaround: Use config-register 0x2102 and unconfigure the clock timezone.

- CSCsu45758

Symptoms: On a Cisco 12000 series router with a dual-RP chassis, the following error message might be raised.

```
Aug 26 04:57:06.885: %REDUNDANCY-3-CONFIG_SYNC: Active and Standby lbl configuration
out of sync
```

Conditions: This symptom is observed when trying to modify the **ip multicast vrf route-limit** commands.

```
Router(config)# ip multicast vrf 13979:6253 route-limit 25
Router(config)# end
Aug 26 04:57:06.885: %REDUNDANCY-3-CONFIG_SYNC: Active and Standby lbl configuration
out of sync
```

Workaround: There is no workaround.

- CSCsu96698

Symptoms: More specific routes are advertised and withdrawn later even if **config aggregate-address net mask summary-only** is configured. The BGP table shows the specific prefixes as suppressed with s>.

Conditions: This symptom occurs only with very large configurations.

Workaround: Configure a distribute-list in the BGP process that denies all of the aggregation child routes.

- CSCsv15835

Symptoms: Traffic running, cell-packing of 5 or more cells, and changing shaping to CBR/VBR-RT on an Engine 3 ATM L2 interface cause the port to exhaust its buffers and all ingress traffic to be dropped.

Conditions: This symptom is observed on a Cisco 12000 router.

Workaround: There is no workaround (you must reload the linecard).

- CSCsv89643

Symptoms: If Ethernet interface configured as Open Shortest Path First (OSPF) point-to-point network then adjacency is being established using only multicast packets. As a result routes calculated over the link do not have MAC address of next-hop's IP resolved prior to routes being installed into the routing table. This leads to delay for routes to become usable as lower-level protocols have to trigger MAC resolution. During short period of time traffic sent over the interface is lost when routes are just installed for the first time.

Conditions: Occurs when Ethernet interface is configured for OSPF point-to-point.

Workaround: Problem will self-correct because passing traffic triggers MAC address resolution.

- CSCsw50410

Symptoms: The following traceback is seen on the console, and all the channelized serial links on the E3 LC flap.

```
SLOT 5:1d00h: %EE48-3-INVALID_CFG_DATA: Channel 4: Invalid configuration data.
Channel type= 5 -Traceback= 40030F00 40417F44 40418208 40418444 404184B4 40418588
SLOT 5:1d00h: %EE48-3-INVALID_CFG_DATA: Channel 5: Invalid configuration data. Channel
type= 5 -Traceback= 40030F00 40417F44 40418208 40418444 404184B4 40418588
```

Conditions: This symptom occurs with all the serial links configured on a Channelized OC48-DS3/Engine 3 card. Serial interfaces flap, bringing down BGP/OSPF for no apparent reason. No configs were done.

Workaround: There is no workaround.

- CSCsw82176

Symptoms: A Cisco 12000 series Internet router that is running Cisco IOS Release 12.0(32)SY7 crashes by Unexpected exception to CPUvector 300.

Conditions: This crash occurs after deleting a couple of subinterfaces that belong to different VRFs. There are many different VRFs and different subinterfaces configured on the router that runs Cisco IOS Release 12.0(32) SY7.

Workaround: Make sure to always shut down the subinterfaces before deleting them.

- CSCsw98681

Symptoms: Given the following topology:

CE1<-->PE1 <---->P<---->PE2<----->CE2

Xconnect is configured on the serial link, and after the following steps are performed, a ping fails for the xconnect interface.

1) Configure xconnect with HDLC encapsulation.

2) Remove the encapsulation and add PPP encapsulation.

Conditions: All interfaces should be up and running.

Workaround: Remove and add the xconnect configuration.

- CSCsx03504

Symptoms: A router CPU stays high (98 to 99 percent) for more than 6 minutes after oif-per-mvrf-limit is set to 2000 lower than the actual total number of OIFs (14000), and all mroute states are re-formed.

Conditions: When oif-per-mvrf-limit is set to a certain number lower than the total number of OIFs in the MVRF.

Workaround: There is no workaround.

- CSCsx06756

Symptoms: Linecards crash.

Conditions: This symptom occurs when a shut/no shut is performed on the SFC card.

Workaround: There is no workaround.

- CSCsx20177

Symptoms: “no int loopback” with “advertise passive-only” causes a stuck prefix.

Conditions: This symptom is observed on a Cisco 7600 series router that is using an RSP720 with Cisco IOS Release 12.2(33)SRD.

Workaround:

- Do not use “advertise passive-only”. Unconfiguring and reconfiguring this command clears the stuck prefix.

Or with “advertise passive-only”:

- First remove “passive-interface loopback” from router isis.
- Then remove the interface via “no int loopback”.

- CSCsx32958

Symptoms: VRF traffic incorrectly routed using default route in global routing table.

Conditions: This problem may occur if a BGP update is received from different route reflectors at different times.

Workaround: There is no workaround.

- CSCsx34297

Symptoms: Watchdog reset seen with combination of NPEG1+PA-POS-1OC3/PA-POS-2OC3.

Conditions: The symptom is observed on a Cisco 7200 series router and on a Cisco 7301 router with an NPEG1 processor.

Workaround: Change the MDL of operation to PULL using the **dma enable pull model** command.
- CSCsx52525

Symptoms: Given a topology as follows:

```
TGN2<---->CE1<---->PE1<---->P<---->PE2<---->CE2<---->TGN2
```

FRoMPLS is configured; PE1 has a dual RP with redundancy mode set to RPR- PLUS. After an RPR + switchover, a few interfaces stop forwarding traffic.

Conditions: All interfaces should be up and running.

Workaround: There is no workaround.
- CSCsx75004

Symptoms: In a Carriers Carrier, the CSC-PE router advertises wrong out-label. This causes the end-to-end LSP to be broken in the CSC network, and all traffic is dropped.

This problem is observed by enabling the **show ip bgp label** command on CSC-CE. See “Out Label” of the route is “imp-null”.

Conditions: This condition is observed in routers that are running Cisco IOS Release 12.0(32)SY6.

Workaround: Configure **neighbor {ip-address | peer- group-name} next-hop-self** on CSC-PE.
- CSCsx78370

Symptoms: Traffic falling into a class where WRED is configured is tail- dropped for no reason. Only PXF traffic is affected; process-switched traffic is not affected (a ping with IP options works).

Conditions: This symptom is observed on a Cisco 10720. It occurs only with Gigabit Ethernet interfaces.

Workaround: Remove the WRED configuration from the policy map.
- CSCsx93485

Symptoms: While redistributing OSPFv3 into BGP, the redistributed route flaps when the OSPFv3 topology changes.

Conditions: This symptom is observed when the cost of the redistributed route becomes better.

Workaround: There is no workaround.

Further Problem Description: As seen from the BGP debugs, RIB sends a DEL and ADD instead of a MODIFY.
- CSCsx94290

Symptoms:

 - 1) In case of a config where police rate is not taking effect on priority command, as we saw it go through default queue. This occurs in a QoS policy with a priority queue where the “police” statement occurs before the priority statement in the policy. Additionally, this occurs only upon the initial configuration of the policy-map. Editing the policy-map will correct the issue.
 - 2) In case of a config where class is configured as only strict priority (no police) and then modified, packets go through non-default and non-priority queue.

Conditions: The initial configuration of policy-map was modified.

Workaround: Detach and re-attach the policy-map.

- CSCsx96402

Symptoms: The LC (E3/E5) crashes upon executing certain **show controller...** commands 3 to 4 times.

Conditions: The symptom is observed with scale configurations on MLPPP, MFR, serial interfaces with features like VRF, VPN, basic QOS, ACL, and NetFlow.

Workaround: There is no workaround.

- CSCsx96600

Symptoms: Policy counters are not updated on the egress of the E5 linecard.

Conditions: This symptom is observed with IPv6 traffic using a Cisco IOS Release 12.0(33)S image. This symptom is not observed with IPv4 traffic.

Workaround: There is no workaround.

- CSCsx97992

Symptoms: An ATM VPWS is configured with an input service policy. While still attached, the service policy (child and parent) is modified. Exiting (Ctrl z) that configuration level results in a crash and a switchover.

Conditions: This symptom is observed under the following conditions:

- You must use SSH (not Telnet) connecting to the router to make the configuration.
- You must attach the input policy to the VC while making the policy-map change.

Workaround: There is no workaround.

- CSCsy22281

Symptoms: Traffic is dropped on an ATM-Redundancy (SR-APS configured) ingress interface.

Conditions: This symptom is observed after an RPR+ switchover is performed.

Workaround: Reload both linecards that are involved in ATM redundancy.

- CSCsy42615

Symptoms: Entries for ABRs and ASBRs are missing from the OSPF route table. This results in inter-area and external routes being omitted from the Routing Information Base (RIB).

Conditions: The bug will only be seen when MPLS-TE tunnels are being used. Also, specifying non-default SPF timer values with **timers throttle spf** will increase the risk of hitting this bug.

Workaround: There is no workaround.

- CSCsy45838

Symptoms: The **show ip ospf border-router** command may cause a router to crash.

Conditions: Occurs if the border table is recalculated in a significant way while the output is being printed on the console. The risk of a crash is reduced if you avoid using the auto-more feature and allow the entire output to display at once.

Workaround: There is no workaround.

- CSCsy60668

Symptoms: On a router in which MPLS Traffic Engineering (TE) is configured, toggling the router-id in the router configuration can cause the router to reload. For example, configuring “router ospf 100 mpls traffic-eng router-id loopback 0” quickly followed by “mpls traffic-eng router-id loopback 1” may trigger this symptom.

Conditions: It is necessary that “mpls traffic-eng tunnel automesh” is running in the OSPF area of the router, although automesh need not be configured on the affected router.

Workaround: There is no workaround.

- CSCsy74390

Symptoms: ISIS adjacency is not established with an E4 SRP linecard.

Conditions: This symptom is observed when ISIS is configured between SRP interfaces with at least one end having an E4 SRP linecard.

Workaround: There is no workaround.

- CSCsy82104

Symptoms: I/O memory leaks after several days. The output of the E1 serial interface may be blocked as well.

Conditions: The symptoms are observed on a Cisco 7200 series router that is running Cisco IOS Release 12.0(33)S and when an E1 interface serial flaps. The QoS outgoing service-policy needs to be provisioned on this serial interface.

Workaround: Remove the outgoing QoS service-policy from the flapped/blocked serial interface.

- CSCsy92142

Symptoms: The serial interface on a channelized OC48 linecard stays in the UP/DOWN state after encountering Layer 1 alarms (PRID or PAIS). The interface continues to be in the UP/DOWN state even after the Layer 1 alarms are cleared.

The interface is configured for PPP encapsulation, and path level delay triggers are enabled on this interface. The link shows UP, but the PPP negotiation will be stuck in Echo Request Sent.

Conditions: This symptom is observed with a 12.0(32)S11o-based image for channelized DS3 Engine 3 linecards with alarm delay triggers configured. The problem will be seen only with momentary path level alarms.

Workaround:

1. Perform a shut/no shut on the serial interface that is in the UP/DOWN state. However, this needs manual intervention every time.
2. Remove the **alarm-delay triggers path 2500** command from the serial interface configuration. However, the side effect of this would cause the serial interface to flap.

- CSCsy94776

Symptoms: A Cisco 12000 series Internet router may have missing Ifib entries on linecards.

Conditions: This symptom is observed in Cisco IOS Release 12.0(32)s11o.

Workaround: Reload the linecard.

- CSCsy96287

Symptoms: A customer experienced a single T1 flapping on controller 0/3/0. It would take between 2,500 and 3,000 path code violations and then drop and come back. It would do this about once every 15 minutes. Problems with our phones losing connectivity to a central call manager when a WAN circuit experiences a problem.

We use Multilink PPP to bundle three T1s for a 4.5-Mb circuit. If any one of the three T1s experiences even a minor issue, phones are resetting. However, we never lose Layer 3 connectivity. The edge router maintains its BGP peering across the Multilink PPP bundle, and none of our management applications ever sees a loss in connectivity.

We recently switched over to Multilink PPP from Multilink Frame due to a requirement by our MPLS provider. We did not have an issue using Multilink Frame; hence, we believe it is an issue with our configuration for Multilink PPP.

Conditions: This issue was first noticed in a 32S6r image, and some nodes running 32s11 showed similar symptoms.

Workaround: Perform a shut/no shut on the serial interface on the Cisco 12000 series side.

Further Problem Description: The root cause of this issue is that the customer was getting exposed to an inherent limitation of a timer that was being used in the T1/E1 line-state processing routine at the PLIM level. The malfunctioning of the timer would result in the PLIM not sending a line-state update message to the linecard and the route processor when a link flapped, and therefore the route processor would not bring the link down even when an alarm was present on the line. This would cause blackholing of traffic for some time until the L2 times out and the protocol comes down.

- CSCsz11893

Symptoms: Some packet loss is observed when traffic is fragmented on a Cisco 12000 series linecard. The issue has been reported using ping packets with a packet size larger than the egress interface MTU size.

Conditions: This symptom is observed on:

- Packets received by the Cisco 12000 series that would require fragmentation on the egress linecard.
- E5 linecards.

Workaround: Change the MTU size to prevent fragmentation from happening on the linecard.

- CSCsz12423

Symptoms: IP-to-MPLS packets that need to be fragmented might be dropped.

Conditions: This symptom is observed when an E4+ line card is used as ingress and an E4+, E5, or E3 line card is used as egress.

Workaround: There is no workaround.

- CSCsz18371

Symptoms: A ping fails for bridging, and spurious access is seen upon reload.

Conditions: This symptom is observed when bridging is configured with HDLC encapsulation on a Cisco 7200 router.

Workaround: There is no workaround.

- CSCsz19255

Symptoms: Tag rewrites are missing on linecards for one of the load-shareable interfaces.

Conditions: This symptom is observed on a Cisco 12000 series router that is running Cisco IOS Release 12.0(32)S11o.

Workaround: Shut/no-shut the interface.

- CSCsz28121

Symptoms: A router crashes when NetFlow export configurations are applied and removed.

Conditions: This symptom is observed only when NetFlow export version 9 configurations are toggled.

Workaround: Use NetFlow export version 5 to export the flows.

- CSCsz33193
Symptoms: For some VCs, traffic is not flowing through the SR-APS interface.
Conditions: This symptom is observed after a linecard reload and router reload.
Workaround: Perform a shut/no shut of the SR-APS interface.
- CSCsz33704
Symptoms: In an FB APS setup, if the protect link has errors and hence signal failure, the APS switches to it when the work link also gets an error.
Conditions: This symptom is observed with a 12.0(32)s11o-based image.
Workaround: There is no workaround.
- CSCsz43391
Symptoms: Traffic stops flowing.
Conditions: This symptom is observed after the following procedure is performed:
 - 1) First try ETH (vlan) to FR over MPLS (traffic is fine).
 - 2) Change the dot1q interface to a QINQ interface on both the PE and the CE.
 - 3) Then change back to dot1q on both the PE and the CE (traffic fails).Workaround: Reload the linecard.
- CSCsz45567
A device running Cisco IOS Software, Cisco IOS XE Software, or Cisco IOS XR Software is vulnerable to a remote denial of service condition if it is configured for Multiprotocol Label Switching (MPLS) and has support for Label Distribution Protocol (LDP).

A crafted LDP UDP packet can cause an affected device running Cisco IOS Software or Cisco IOS XE Software to reload. On devices running affected versions of Cisco IOS XR Software, such packets can cause the device to restart the mpls_ldp process.

A system is vulnerable if configured with either LDP or Tag Distribution Protocol (TDP).

Cisco has released free software updates that address this vulnerability.

Workarounds that mitigate this vulnerability are available.

This advisory is posted at:
<http://www.cisco.com/warp/public/707/cisco-sa-20100324-ldp.shtml>
- CSCsz46285
Symptoms: MVPN traffic is punted to the line-card CPU.
Conditions: This symptom is observed on the decap side of data mdt traffic.
Workaround: There is no workaround.
- CSCsz58546
Symptoms: In APS, in Choc48 LC, APS switching from protect to work is not happening when SF is present on a protect link and SD is present on a work link.
Conditions: All interfaces should be up and running.
Workaround: There is no workaround.

- CSCsz70552

Symptoms: On the “P” router with four POS links, where two links are working as the primary and two links are working for redundancy; after a telco issue, both POS links go down due to transmission problems. The trigger for this issue is both links going down.

The P router sets LIB local binding changes to implicit null for several prefixes. After that, the PE routers have connectivity issues in some VRFs and do not go through a backup path using POS interface.

Looking into the PE routers that are connected to this P router, the following deviation was observed in their LFIB tables:

```
Router_PE# sh mpls for 10.38.193.192 de
```

```
Local Outgoing Prefix Bytes tag Outgoing Next Hop tag tag or VC or Tunnel Id switched
interface 37 Pop tag 10.38.193.192/32 0 Gi3/0 10.125.93.222 MAC/Encaps=30/30,
MRU=1530, Tag Stack{} 00000000000000000000000010100000000055FFF99FE000197D0ED808847 No
output feature configured
```

```
Router_PE# sh ip cef 10.38.193.192 de
```

```
10.38.193.192/32, version 72378, epoch 0, cached adjacency 10.125.93.222 0 packets, 0
bytes tag information set, shared, all rewrites owned local tag: 37 via 10.125.93.222,
GigabitEthernet3/0, 3 dependencies next hop 10.125.93.222, GigabitEthernet3/0 valid
cached adjacency tag rewrite with Gi3/0, 10.125.93.222, tags imposed {}
```

It looks as though the P router sends a pop to the PE routers.

Conditions: This symptom is observed under the following conditions:

- The P router has two links to the primary path and two links to the backup path.
- PPP encapsulation is used.

Workaround:

- Change from PPP to HDLC encapsulation on the POS links.
- Enter the “clear ip route <prefix>” command.

Or

- Enter the “clear ip route *” command.

- CSCsz71787

Symptoms: A router crashes when it is configured with DLSw.

Conditions: A vulnerability exists in Cisco IOS software when processing UDP and IP protocol 91 packets. This vulnerability does not affect TCP packet processing. A successful exploitation may result in a reload of the system, leading to a denial of service (DoS) condition.

Cisco IOS devices that are configured for DLSw with the `<cmd>dlsw local- peer</cmd>` automatically listen for IP protocol 91 packets. A Cisco IOS device that is configured for DLSw with the `<cmd>dlsw local-peer peer-id <IP- address></cmd>` command listen for IP protocol 91 packets and UDP port 2067.

Cisco IOS devices listen to IP protocol 91 packets when DLSw is configured. However, it is only used if DLSw is configured for Fast Sequenced Transport (FST). A DLSw FST peer configuration will contain the following line:

```
<cmd>dls w remote-peer 0 fst <ip-address></cmd>
```

It is possible to disable UDP processing in DLSw with the `dls w udp-disable` command. However, disabling UDP only prevents the sending of UDP packets; it does not prevent the device from receiving and processing incoming UDP packets.

Workaround: The workaround consists of filtering UDP packets to port 2067 and IP protocol 91 packets. Filters can be applied at network boundaries to filter all IP protocol 91 packets and UDP packets to port 2067, or filters can be applied on individual affected devices to permit such traffic only from trusted peer IP addresses. However, since both of the protocols are connectionless, it is possible for an attacker to spoof malformed packets from legitimate peer IP addresses.

As soon as DLSw is configured, the Cisco IOS device begins listening on IP protocol 91. However, this protocol is used only if DLSw is configured for Fast Sequenced Transport (FST). A DLSw FST peer configuration will contain the following line:

```
<cmd>dls w remote-peer 0 fst <ip-address></cmd>
```

If FST is used, filtering IP protocol 91 will break the operation, so filters need to permit protocol 91 traffic from legitimate peer IP addresses.

It is possible to disable UDP processing in DLSw with the `dls w udp-disable` command. However, disabling UDP only prevents the sending of UDP packets; it does not prevent the receiving and processing of incoming UDP packets. To protect a vulnerable device from malicious packets via UDP port 2067, both of the following actions must be taken:

1. Disable UDP outgoing packets with the `dls w udp-disable` command. And
2. Filter UDP 2067 in the vulnerable device using infrastructure ACL.

*** Using Control Plane Policing on Affected Devices**

Control Plane Policing (CoPP) can be used to block untrusted DLSw traffic to the device. Cisco IOS software releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP may be configured on a device to protect the management and control planes to minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic sent to infrastructure devices in accordance with existing security policies and configurations. The following example, which uses 192.168.100.1 to represent a trusted host, can be adapted to your network. If FST is not used, protocol 91 may be completely filtered. Additionally, if UDP is disabled with the `dls w udp-disable` command, UDP port 2067 may also be completely filtered.

```
!--- Deny DLSw traffic from trusted hosts to all IP addresses
!--- configured on all interfaces of the affected device so that
!--- it will be allowed by the CoPP feature.

access-list 111 deny udp host 192.168.100.1 any eq 2067
access-list 111 deny 91 host 192.168.100.1 any

!--- Permit all other DLSw traffic sent to all IP addresses
!--- configured on all interfaces of the affected device so that it
!--- will be policed and dropped by the CoPP feature.

access-list 111 permit udp any any eq 2067
access-list 111 permit 91 any any

!--- Permit (Police or Drop)/Deny (Allow) all other Layer 3 and Layer 4
!--- traffic in accordance with existing security policies and
!--- configurations for traffic that is authorized to be sent
!--- to infrastructure devices.
!--- Create a Class-Map for traffic to be policed by
!--- the CoPP feature.

class-map match-all drop-DLSw-class
 match access-group 111

!--- Create a Policy-Map that will be applied to the
!--- Control-Plane of the device.
```

```

policy-map drop-DLSw-traffic
  class drop-DLSw-class
    drop
!--- Apply the Policy-Map to the Control-Plane of the
!--- device.
control-plane
  service-policy input drop-DLSw-traffic

```

In the above CoPP example, the access control entries (ACEs) that match the potential exploit packets with the “permit” action result in these packets being discarded by the policy-map “drop” function, while packets that match the “deny” action (not shown) are not affected by the policy-map drop function. Please note that in the Cisco IOS 12.2S and 12.0S trains, the policy-map syntax is different:

```

policy-map drop-DLSw-traffic
  class drop-DLSw-class
    police 32000 1500 1500 conform-action drop exceed-action drop

```

Additional information on the configuration and use of the CoPP feature is available at:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod_white_paper0900aecd804fa16a.html

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrtlmt.html

* Using Infrastructure ACLs at Network Boundary

Although it is often difficult to block traffic transiting your network, it is possible to identify traffic that should never be allowed to target your infrastructure devices and block that traffic at the border of your network. iACLs are a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for this specific vulnerability. The iACL example shown below should be included as part of the deployed infrastructure access-list that will protect all devices with IP addresses in the infrastructure IP address range. If FST is not used, protocol 91 may be completely filtered. Additionally, if UDP is disabled with the dlsu udp-disable command, UDP port 2067 may also be completely filtered.

```

!--- Permit DLSw (UDP port 2067 and IP protocol 91) packets
!--- from trusted hosts destined to infrastructure addresses.
access-list 150 permit udp TRUSTED_HOSTS MASK INFRASTRUCTURE_ADDRESSES MASK eq 2067
access-list 150 permit 91 TRUSTED_HOSTS MASK INFRASTRUCTURE_ADDRESSES MASK
!--- Deny DLSw (UDP port 2067 and IP protocol 91) packets from
!--- all other sources destined to infrastructure addresses.
access-list 150 deny udp any INFRASTRUCTURE_ADDRESSES MASK eq 2067
access-list 150 deny 91 any INFRASTRUCTURE_ADDRESSES MASK
!--- Permit/deny all other Layer 3 and Layer 4 traffic in accordance
!--- with existing security policies and configurations.
!--- Permit all other traffic to transit the device.
access-list 150 permit ip any any
interface serial 2/0
  ip access-group 150 in

```

The white paper entitled “Protecting Your Core: Infrastructure Protection Access Control Lists” presents guidelines and recommended deployment techniques for infrastructure protection access lists. This white paper can be obtained at the following link:

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml

Further Problem Description: This vulnerability occurs on multiple events to be exploited. It is medium complexity in order to exploit and has never been seen in customers environment.

- CSCsz72591
Symptoms: A router crashes with an Address Error (load or instruction fetch) exception.
Conditions: The router must be configured to act as a DHCP client.
Workaround: There is no workaround.
- CSCsz78479
Symptoms: When the PE routes traffic with a default network, it suddenly stops forwarding the packets from the CE. The PE is still able to reach the Internet.
Conditions: The PE is configured with the **ip default network** command and has an Engine 5.
Workaround: Remove and re-add the **ip default network** command.
Further Problem Description: The issue was already reproduced on the CALO case.
- CSCsz81356
Symptoms: E6 linecards crash immediately after a CSC switchover.
Conditions: The CSC switchover is caused by a CSC card failure or by the CLI shutting down the primary CSC.
Workaround: There is no workaround.
- CSCsz84906
Symptoms: The ISIS redistribution RIB has a stale route that is not removed after the original ISIS route is deleted when an interface is shut down. This can cause wrong ISIS database information and wrong routing information in the routing table.
Conditions: This symptom is observed when the router is an L1L2 router and the old ISIS route to be deleted after interface shutdown has a backup route from other routing protocols. If the **ip routing protocol purge interface** command is configured, the issue will not happen.
Workaround: Either configure the **ip routing protocol purge interface** command or enter the **clear isis *** command, which may resolve the problem temporarily.
- CSCsz89090
Symptoms: When the **delay triggers line** command is executed under a controller, the configured values are not reflected in the running configuration.
Conditions: This symptom is observed in Cisco IOS Release 12.0(33)S and 12.0 (32)SY9 images.
Workaround: There is no workaround.
- CSCsz89107
Symptoms: CPU utilization is high when there is a scaled configuration of more than 1000 interfaces and 100-pps traffic is being sent on UUT along with BGP and multicast traffic.
Conditions: This symptom is observed when several sessions are active and generating traffic.
Workaround: There is no workaround.
- CSCta08632
Symptoms: After supervisor forces switchover several times, a router two hops away has wrong ISIS topology and ISIS routing table.
Conditions:
 1. Incremental shortest path first (ISPF) enabled in ISIS.
 2. **set-overload-bit** on-startup in ISIS.

3. Supervisor force switchover several times

Workaround: Disable ISPF in ISIS.

- CSCta24441

Symptoms: Under certain circumstances, an E5 linecard may stop forwarding traffic to a certain subinterface. We see ARP entries updated, but traffic is not arriving on the connected equipment. Accordingly, we see on the connected equipment that ARP ages out. The connected VLAN becomes isolated to the rest of the network. Also, control protocols on the affected interface can go down.

Conditions: The Cisco 12000 is connected to a dot1q trunk. The issue is seen on subinterfaces with or without VRF, and with various lengths of subnet masks. This issue is seen when the adjacencies of the affected interface have an adjacency index with a value greater than 16383. This issue can be seen in a scaled testbed where there is a lot of churn in adjacency creation and deletion as a result of subinterface deletion and creation or ARP entries getting timed-out and refreshed.

Workaround: Perform a shut/no shut on the subinterface. Make sure to pause before bringing the subinterface back up. If this does not work, remove the subinterface and configure the same again.

If the above workaround does not work, reloading the RP is the only solution.

- CSCta25677

Symptoms: Upon an RPR+ switchover, a few MLPPP interfaces that are configured on an E3 1xChOC12 may start having ping failures.

Conditions: This symptom is observed with a Cisco IOS 12.0(32)S11p fc1 image.

Workaround: Perform a shut/no-shut on the ML interface.

- CSCta30330

Symptoms: PIM checksum errors are causing the joins to be dropped in the MVPN.

Conditions:

Topology _____

ce3-----BR(Pe)(IOS-XR)-----Pe1(IOS)-----source

Initially, we observed a null olist in the VRF mroutes on the Cisco IOS router. Ideally, in this case, a tunnel should have been there in the olist.

Then we checked if the tunnel joins are sent and received by the Cisco IOX and IOS routers, respectively, by enabling the PIM debugs on both routers.

The XR debugs confirmed that joins are sent out by the XR node. Then we checked the debugs on the Cisco IOS router.

Initially, we suspected that the problem is due to “not to us” messages. Then we checked the IP traffic statistics.

PE1# **show ip traffic**

```
IP statistics: >>>> PIMv2 statistics: Sent/Received Total: 2087399/4842053, 245046
checksum errors, 0 format errors Registers: 0/0, Register Stops: 0/0, Hellos:
571945/560676 Join/Prunes: 1515499/4036576, Asserts: 0/0, grafts: 0/0 Bootstraps: 0/0,
Candidate_RP_Advertisements: 0/0 Queue drops: 0
PIMv2 statistics: Sent/Received Total: 2092509/4848529, 245374 checksum errors, 0
format errors Registers: 0/0, Register Stops: 0/0, Hellos: 573425/561965 Join/Prunes:
1519100/4041190, Asserts: 0/0, grafts: 0/0 Bootstraps: 0/0,
Candidate_RP_Advertisements: 0/0 Queue drops: 0
PIMv2 statistics: Sent/Received Total: 2092834/4848711, 245396 checksum errors, 0
format errors Registers: 0/0, Register Stops: 0/0, Hellos: 573515/562041 Join/Prunes:
1519335/4041274, Asserts: 0/0, grafts: 0/0 Bootstraps: 0/0,
Candidate_RP_Advertisements: 0/0 Queue drops: 0 >>>>
```

We observed checksum errors.

Workaround: After seeing checksum errors in the IP traffic statistics, we tried shutting the core-facing interface in the olist. After that, the problem disappeared. When we added that interface back, the problem was reproduced again. We suspect the following to cause this issue.

When we have core and VRF interfaces on the egress LC (E5), the PIM packet has to be forwarded on the core-facing interface and also has to be punted to the RP. In the E5, this is done by recycling the packet. In the first cycle, the packet will be sent to the core interface; in the second cycle, the packet will be decapsulated and punted to the LC CPU.

Only the head gets recycled for different passes. The tail will be stored in the stingray. When the packet is punted to the LC CPU, the LC CPU will copy the tail from the stingray, attach it to the head, and send it to the RP. We suspect that this copy is not happening properly and the RP is seeing PIM checksum errors.

- CSCta37296

Symptoms: On a Cisco 12000 ATM linecard, threshold drops are observed on a service policy that is configured with WRED, and these drops occur even if no random drops are incrementing.

Conditions: This symptom is observed only when using WRED, and it is observed even under low utilization of the service policy. Threshold drops will happen only for RP-generated packets even though there are no random drops.

Workaround: To stop the drops, remove WRED and configure a standard queue limit.

Further Problem Description: Some of the packet types that are generated by the linecard (such as ICMP echo response) will still undergo threshold drops.

- CSCta45402

Symptoms: In an MVPN setup with a CE connected via an MLPPP interface, auto- RP packets are not being punted to the RP and the RP entry times out after 180 seconds.

Conditions: This symptom is observed either when a link flaps on a member of the MLPPP interface or when output QoS is applied on the MLPPP interface.

Workaround:

- 1) RP# **clear ip mroute vrf <vpn> 224.0.1.40**
- 2) LC# **clear ip mds all**
- 3) Configure static RP.
- 4) Remove the output policy on the outgoing Multilink.

- CSCta58995

Symptoms: A Cisco 7200 PE is dropping *small* frames on an AToM FRoMPLS tunnel.

Conditions: This symptom is observed in an FR IP IW case when frames that are less than 60 bytes are sent from a Cisco 12000 series router (PE on the other side).

Workaround: There is no workaround.

- CSCta69919

Symptoms: On a Cisco 12000 series router with ISE line cards and an IPv6 ACL, after a reload or RP switchover, the ACL does not match traffic correctly.

Conditions: This applies to IPv6 ACL.

Workaround: Delete and recreate the ACL.

- CSCta76975

Symptoms: IPv6 multicast traffic drops are observed when IPv6 multicast traffic is sent at a high rate. These multicast packets are punted to the RP; this can be seen through the `show ipv6 mflib <multicast address> CLI`.

Conditions: This symptom is observed upon router reload.

Workaround: There is no workaround.

- CSCta77678

Symptoms: RTP timestamp on the RFC 2833 event is modified. IP Phones are using RFC 2833 to transport the DTMF signals, which causes problems with the voicemail systems.

Conditions: This symptom occurs when RTP header compression is enabled.

Workaround: There is no workaround.

Further Problem Description: The problem disappears if cRTP is disabled. The issue is seen with Class-Based cRTP configured and also with other cRTP configuration types.

- CSCtb08699

Symptoms: The traffic flow between the Cisco 12000 series PE routers and the core CRS router stopped unexpectedly without any trigger, and the linecard had to be reloaded for recovery.

Conditions: The packet buffers in the ingress direction of the core-facing linecards of the Cisco 12000 series were gradually being depleted. Once this happened, all the incoming packets were dropped as seen in “no mem drop” below:

```
LC-Slot1# show contr tofab qm stat
```

```
135590 no mem drop, 193180 soft drop, 4167963929 bump count 0 rawq (High Priority)
drops, 0 rawq (Medium Priority) drops, 0 rawq (Low Priority) drops 0 dnq1 drops, 0
dnq2 drops 0 no memory (ns), 0 no memory hwm (ns) no free queue 0 126499 61990 15125
36 0 0 0 0 0 0 0 0 0 0 0
```

Workaround:

- 1) Clear the corrupted entry using the “clear ip route vrf <vpn-name> <prefix>” command on the RP.
- 2) Reload the linecard.
- 3) Reclaim the lost buffers by forced re-carve.

- CSCtb45062

Symptoms: A subinterface does not transmit traffic in the egress direction, the queue head and tail stay frozen, and the txport is consistently back- pressured.

Conditions: These symptoms are observed under the following conditions:

- 12000-SIP-501 with SPA-8X1FE-TX-V2.
- One Fast Ethernet interface with more than 468 subinterface VLANs.
- All subinterfaces with the same policy (SHAPE_OUT_960).

```
policy-map VBL class
  class-default
    police cir 96000 bc 4470 be 4470 conform-action set-dscp-transmit af11
  exceed-action
  set-dscp-transmit default
policy-map SHAPE_OUT_960
  class class-default
    shape average 960000
  service-policy VBL
```

Workaround: Create a dummy Fast Ethernet subinterface and force it to allocate the tx-port being back-pressured.

Further Problem Description: Removing the policy and re-applying it or performing a shut/no shut solves the issue temporally, but the issue will move to another subinterface in the same main interface.

- CSCtb49864

Symptoms: An HP ingress policy is applied on the Gigabit Ethernet main interface (E5). After an RP switchover, the counter for the “show policy-map int gig 0/0/0” command stays at 0 even though the police function appears to be working okay. The policer also disappears from the “show policy-map int” command output.

Conditions: RP switchover.

Workaround:

1. Perform a shut/no shut on the interface.
2. Delete/re-apply the service policy on the interface.

- CSCtb51864

Symptoms: An IPv6 ACL is not working on the ingress of an E3 engine.

Conditions: Apply the IPv6 ACL on the ingress of the E3 engine, remove the ACL, and then reapply the same ACL on the same interface.

Workaround: Reload the linecard.

- CSCtb52229

Symptoms: When a class map is added to an existing service policy (with a huge number of class maps), high CPU utilization occurs and CPU hog messages are seen, which causes OSPF flapping, and, in turn, a network outage.

Conditions: This symptom is observed when a class map is bonded/unbonded from a service policy that has a huge number of class maps.

Workaround: There is no workaround.

- CSCtc36576

Symptoms: In a FR-Ethernet IP interworking scenario, a Cisco 12000 series PE (with an E5 linecard being used as CE facing) corrupts CE-to-CE packets that are less than 58 bytes.

Conditions: One Cisco 12000 series is running Cisco IOS Release 12.0(32) SY8, 12.0(32)SY9, or 12.0(32)SY10. The linecard that is facing the CE must be E5.

Workaround: There is no workaround.

- CSCtc55200

Symptoms: An E5 linecard crashes while the “show ip hardware-cef x.x.x.x detail” command is executed during CEF troubleshooting.

Conditions: This symptom is observed under the following conditions:

- Core-facing interfaces using Eng3 with two Port-Channel and load-balance.
- Customer-facing interfaces using Eng5 with exhausted FSRAM memory because of a high number of hosts or load-balance routes from Eng3.

When FSRAM memory becomes exhausted, if you try to add one more host on the port-channel, the following error message will appear:

```
SLOT 4:02:04:44: %EE192-3-LINKBUNDLE: Cannot create hw link_bundle -Traceback=
40030EE8 4068CAC8 405AF138 413B6CCC 413D7464 413D7FA0 413BB2F4 413BB580 413BB88C
413BC780
```

Workaround: Reload the linecard.

- CSCtc72808

Symptoms: In situations where an enhanced SFC module would experience problems with the clock module, a recovery feature that was introduced in previous releases would try to recover switch fabric system indefinitely:

```
%FABRIC-3-ERR_HANDLE: Reconfigure all fabric cards due to SUSHI REGISTER RESET ERROR
error from slot <..>
```

And that would lead to linecard resets in the chassis.

Conditions: This behavior is observed when a enhanced SFC module experiences hardware/clock module problems.

Workaround: Disable the faulty module in configuration mode:

```
hw-module slot <slot> shutdown
```

- CSCtc76700

Symptoms: An E5 T1E1 SPA loses all configurations when the image is loaded.

Conditions: This symptom is observed when the latest Cisco IOS Release 12.0 (33)S6 image is loaded.

Workaround: There is no workaround.

- CSCtd15620

Symptoms: An interface on a ChOC12 linecard remains down after a shut/no shut is performed.

Conditions: This symptom is observed when a shut/no shut is performed on a serial interface.

Workaround: Perform a shut/no shut on the SONET controller.

Resolved Caveats—Cisco IOS Release 12.0(33)S5

All the caveats listed in this section are resolved in Cisco IOS Release 12.0(33)S5. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCsx70889

Cisco devices running affected versions of Cisco IOS Software are vulnerable to a denial of service (DoS) attack if configured for IP tunnels and Cisco Express Forwarding. Cisco has released free software updates that address this vulnerability. This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090923-tunnels.shtml>.

- CSCsz55293

Symptoms: A remote third-party device is resetting the IPv6 BGP session with a Cisco 12000 router.

Conditions: BGP is exchanging only IPv6 capability with the remote EBGP peer, but IPv4 capability will be enabled by default. The remote EBGP peer is sending only IPv6 capability, and we should advertise only IPv6 prefixes because that is the capability negotiated. We are wrongly marking IPv4 capability as negotiated and advertising IPv4 prefixes, and the remote neighbor is resetting the session because IPv4 capability is not negotiated at the peer end.

Workaround: Configure a route map to deny all IPv4 prefixes, and apply it as follows:

```
Route-map deny-ipv4 deny 10
```

```
Router bgp <asnum>
address-family ipv4
Neighbor <IPv6Address> activate
Neighbor <IPv6Address> route-map <deny-ipv4> out
```

- CSCta24441

Symptoms: Under certain circumstances, an E5 linecard may stop forwarding traffic to a certain subinterface. We see ARP entries updated, but traffic is not arriving on the connected equipment. Accordingly, we see on the connected equipment that ARP ages out. The connected VLAN becomes isolated to the rest of the network. Also, control protocols on the affected interface can go down.

Conditions: The Cisco 12000 is connected to a dot1q trunk. The issue is seen on subinterfaces with or without VRF, and with various lengths of subnet masks. This issue is seen when the adjacencies of the affected interface have an adjacency index with a value greater than 16383. This issue can be seen in a scaled testbed where there is a lot of churn in adjacency creation and deletion as a result of subinterface deletion and creation or ARP entries getting timed-out and refreshed.

Workaround: Perform a shut/no shut on the subinterface. Make sure to pause before bringing the subinterface back up. If this does not work, remove the subinterface and configure the same again.

If the above workaround does not work, reloading the RP is the only solution.

- CSCta33973

Recent versions of Cisco IOS Software support RFC4893 (“BGP Support for Four-octet AS Number Space”) and contain two remote denial of service (DoS) vulnerabilities when handling specific Border Gateway Protocol (BGP) updates.

These vulnerabilities affect only devices running Cisco IOS Software with support for four-octet AS number space (here after referred to as 4-byte AS number) and BGP routing configured.

The first vulnerability could cause an affected device to reload when processing a BGP update that contains autonomous system (AS) path segments made up of more than one thousand autonomous systems.

The second vulnerability could cause an affected device to reload when the affected device processes a malformed BGP update that has been crafted to trigger the issue.

Cisco has released free software updates to address these vulnerabilities.

No workarounds are available for the first vulnerability.

A workaround is available for the second vulnerability.

This advisory is posted at the following link:

<http://www.cisco.com/warp/public/707/cisco-sa-20090729-bgp.shtml>

Resolved Caveats—Cisco IOS Release 12.0(33)S4

All the caveats listed in this section are resolved in Cisco IOS Release 12.0(33)S4. This section describes only severity 1, severity 2, and select severity 3 caveats.

Basic System Services

- CSCsw76894

Symptoms: IPv6 traps are not sent. And sometimes “%IP_SNMP-3-SOCKET: can't open UDP socket” messages can also be seen.

Conditions: This symptom is observed when no IPv4 address is configured.

Workaround: Perform the following three steps:

1. Disable the SNMP engine by issuing the **no snmp-server** command.
2. Configure an IP address and an IPv6 address on loopback interfaces.
3. Enable the SNMP engine.

- CSCsz87312

Symptoms: A Cisco 12000 series Internet router that is running Cisco IOS Release 12.0(33)S3 may have partial debug outputs of the **debug snmp packet** command in the log even though no such **debug** command is enabled.

The edited log would appear as follows:

<snip>

May 27 15:36:52.272 UTC: SNMP: Packet sent via UDP to xxx.xxx.xxx.xxx

<snip>

Conditions: The messages appear because of a reply to an SNMP probe.

Workaround: There is no workaround.

Further Problem Description: This symptom is not observed in Cisco IOS Release 12.0(33)S2.

Resolved Caveats—Cisco IOS Release 12.0(33)S3

All the caveats listed in this section are resolved in Cisco IOS Release 12.0(33)S3. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCdw62064

Symptoms: Inbound data packets that are reassembled from multilink fragments may not be processed properly on Multilink PPP (MLP) interfaces that are receiving encrypted IP Security (IPSec) traffic that is terminated locally when a hardware accelerator is used for decryption.

Conditions: This symptom affects all inbound reassembled data frames that are received by the bundle and not just those data frames that are carrying encrypted IP datagrams. Most significantly, inbound Internet Security Association and Key Management Protocol (ISAKMP) keepalives are not processed, leading to the eventual failures of the associated IPSec sessions.

The IPSec sessions are reestablished after each failure, but traffic drops will occur until the session is renegotiated via the Internet Key Exchange (IKE). Thus, the observable symptoms are an intermittent failure of IPSec sessions combined with high loss rates in the encrypted data traffic.

Workaround: Disable hardware crypto acceleration, and use software crypto acceleration instead.

- CSCed55180

Symptoms: After a Stateful Switchover (SSO) occurs on a Cisco 7500 series, the traffic interruption may last longer than you would expect.

Conditions: This symptom is observed on Cisco 7500 series that runs Cisco IOS Release 12.2(22)S and that is configured with a Route Switch Processor 4 or 8 (RSP4 or RSP8) when the router is configured with a large number (100,000) of Border Gateway Protocol (BGP) routes and Ethernet interfaces that process traffic.

Workaround: There is no workaround. One way to help reduce the length of the traffic interruption is to add static ARP entries.

- CSCei45749

Symptoms: When you enter the **clear interface** command on an Inverse Multiplexing for ATM (IMA) interface configured for dynamic bandwidth, the PVCs that are associated with the IMA interface may become Inactive.

Conditions: This symptom is observed only for IMA interfaces that have the **atm bandwidth dynamic** command enabled.

Workaround: Issuing the **no atm bandwidth dynamic** command from the IMA interface can prevent the problem from happening. If the problem has been experienced already, using the **no atm bandwidth dynamic** command followed by a **shutdown** and subsequent **no shutdown** from the IMA interface can be used to work around the problem and clear the inactive PVC condition.

- CSCek77589

Symptoms: The following message is observed in syslog/console.

```
%UTIL-3-IDTREE_TRACE: SSM SEG freelist DB:Duplicate ID free
```

Conditions: This symptom was observed during scalability testing of a large number (over 2000) of PPP sessions being brought up and torn down continuously.

Workaround: There is no workaround.

- CSCir01027

Symptoms: SNMP over IPv6 does not function.

Conditions: This symptom is observed on a Cisco router that integrates the fix for caveat CSCsg02387. A list of the affected releases can be found at <http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsg02387>. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

Workaround: Use SNMP over IPv4.

- CSCsd23579

Symptoms: On PPP links that do not support duplicate address detection (DAD), the interface up state can be signaled too early, for example before the interface is actually up. As a result, OSPFv3 neighbor relationship is not established.

Conditions: Any interface that does not support DAD could signal link local up before the interface is up.

Workaround: There is no workaround.

- CSCsd47863

Symptoms: Summary Refresh messages are not sent downstream; consequently, the downstream router notices missing refreshes, and, after some time, the tunnel goes down.

Conditions: This symptom is observed when there is an alternate FRR path and it becomes active. The router that has refresh reduction enabled creates the problem. The command that creates the problem is:

ip rsvp signalling refresh reduction

Workaround: Disable Refresh Reduction on the router using the following command:

no ip rsvp signalling refresh reduction

Further Problem Description: When an incoming interface on a router is shut down, FRR is triggered, and tunnels takes another path.

Now the Path messages on this router come via a different incoming interface. This router had **ip rsvp signalling refresh reduction** enabled.

We can now see that this router stops sending Refresh reduction messages downstream. After some time, the downstream router will say that it has missed the refreshes and then after some time (around 5 minutes), the tunnel will be down.

- CSCsf04035

Symptoms: Upon an SSO switchover, on the new active RP, the MFR interface shows the default bandwidth value instead of the actual bandwidth, which is based on the available bundle links.

Conditions: This symptom is observed on a Cisco 7600 router that is running 12.2SR software and on a Cisco 12000 series Internet router that is running 12.0SY software.

Workaround: Recycle the MFR interface to reset the bandwidth to the correct value.

- CSCsf32449

Symptoms: A Sup720 Multicast-VPN (MVPN) PE router may not advertise its mdt prefix (BGP vpnv4 RD-type 2) after reloading.

Conditions: This symptom is observed on a Sup720 MVPN PE router.

Workaround: Use the **clear ip bgp** command after reloading.

- CSCsg00102

Symptoms: SSLVPN service stops accepting any new SSLVPN connections.

Conditions: A device configured for SSLVPN may stop accepting any new SSLVPN connections, due to a vulnerability in the processing of new TCP connections for SSLVPN services. If the **debug ip tcp transactions** command is enabled and this vulnerability is triggered, debug messages with connection queue limit reached will be observed.

This vulnerability is documented in two separate Cisco bug IDs, both of which are required for a full fix CSCso04657 and CSCsg00102.

- CSCsg02387

Symptoms: A time-out occurs when you enter an SNMP command for an IPv6 interface. However, you can ping the IPv6 interface.

Conditions: This symptom is observed on a Cisco 7200 series but is platform-independent.

Workaround: There is no workaround.

- CSCsh97579

Cisco devices running affected versions of Cisco IOS Software are vulnerable to a denial of service (DoS) attack if configured for IP tunnels and Cisco Express Forwarding. Cisco has released free software updates that address this vulnerability. This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090923-tunnels.shtml>.

- CSCsi57031

Symptoms: On a pseudowire that is configured on an OC-12 ATM interface, when you delete the **oam-ac emulation-enable** command, enter the **write memory** command, and then initiate an SSO switchover, the new standby PRE continues to reboot because of a configuration mismatch with the new active PRE.

Conditions: This symptom is observed on a Cisco 10000 series when the new active PRE has the **oam-ac emulation-enable** command in its configuration but the new standby PRE does not, causing a configuration mismatch. The symptom may not be platform-specific.

Workaround: Reload the new active PRE, then remove the **oam-pvc manage 0** command from its configuration.

- CSCsj56281

Symptoms: Inherit peer-policy does not work.

Conditions: This symptom is observed after a router reload

Workaround: There is no workaround.

- CSCsj60462

Symptoms: Unicast traffic is multicasted.

Conditions: This symptom is observed if two sources send traffic at the same time.

Workaround: There is no workaround.

- CSCsj75907

Symptoms: Traffic may be lost, and the port mode VC goes down.

Conditions: This symptom is observed when an OIR is performed on the PE edge interface in an L2VPN setup.

Workaround: Reset the interfaces on the PEs.

- CSCsj88665

Symptoms: A device with a PA-MC-2T3+ may reset because of a bus error if a channel group is removed while the **show interface** command is being used from another telnet session at the same time, and then the telnet session is cleared.

The device may also display Spurious Memory Accesses.

Conditions: These symptoms have been observed in the latest Cisco IOS 12.4T and 12.2S releases.

Workaround: Do not remove a channel group while using the **show interface** command for that interface.

- CSCsk27147

Symptoms: The following SNMP is incorrectly generated:

```
%SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
```

This issue is affecting the CISCO-MEMORYPOOL-MIB instead.

Conditions: Occurs on a Cisco 2600 series router running Cisco IOS Release 12.4(11)T3. The router keeps dropping SNMP packets. The log shows that the packets are dropped because of the input queue being full. Although the utilization is sometimes high, this could not be the root cause, as the router keeps dropping packets regardless of the current utilization. Also, the SNMP process takes 5 to 20 percent of the CPU load.

Workaround: Exclude ciscoMemoryPoolMIB from your query with the following commands:

snmp-server view public-view iso included

snmp-server view public-view ciscoMemoryPoolMIB excluded

Apply this view to the RW community string. This view will exclude only ciscoMemoryPoolMib, all other MIBs will be available.

- CSCsk31502

Symptoms: A router that is running IPv6 in IP tunnelling may reload upon receiving a malformed packet.

Conditions: The router needs to be configured for IPv6 in IP tunneling.

Workaround: There is no workaround.

- CSCsk59579

Symptoms: The error message “eelc_add_a_port_to_root: port number not contiguous” is displayed, and SPAs may eventually go out of service.

Conditions: This symptom is observed under a race condition due to a back-to-back removal and addition of a member from the bundle.

Workaround: Shut down the member before removing it from the bundle.

- CSCsk64158

Several features within Cisco IOS Software are affected by a crafted UDP packet vulnerability. If any of the affected features are enabled, a successful attack will result in a blocked input queue on the inbound interface. Only crafted UDP packets destined for the device could result in the interface being blocked, transit traffic will not block the interface.

Cisco has released free software updates that address this vulnerability.

Workarounds that mitigate this vulnerability are available in the workarounds section of the advisory.

This advisory is posted at the following link:

<http://www.cisco.com/warp/public/707/cisco-sa-20090325-udp.shtml>

- CSCsk78809

Symptoms: If the traffic flow is re-routed a couple of times due to routing information changes under a heavy load, the linecard suddenly stops forwarding traffic, and then even if the utilization is zero, the linecard does not forward packets anymore.

Conditions: This problem is specific to SPA-1X10GE-L-V2 cards. It is associated with a failed re-initialization of the SPA; that is, the problem can be reproduced by re-initializing the SPA while traffic is artificially sent to the SPA rx side during the re-initialization. Traffic is IMIX with giant/jumbo packets.

Workaround: There is no workaround. The proper operations can be recovered via “reload slot x.”

- CSCsl49628

Symptoms: When a VPN routing/forwarding (VRF) is deleted through the CLI, the VRF deletion never completes on the standby RP, and the VRF cannot be reconfigured at a later time.

Conditions: This symptom is observed when BGP is enabled on the router.

Workaround: There is no workaround.

- CSCsm27071

A vulnerability in the handling of IP sockets can cause devices to be vulnerable to a denial of service attack when any of several features of Cisco IOS Software are enabled. A sequence of specially crafted TCP/IP packets could cause any of the following results:

- The configured feature may stop accepting new connections or sessions.
- The memory of the device may be consumed.
- The device may experience prolonged high CPU utilization.
- The device may reload.

Cisco has released free software updates that address this vulnerability.

Workarounds that mitigate this vulnerability are available in the “workarounds” section of the advisory.

The advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090325-ip.shtml>.

- CSCsm49112

Problem Description: When eBGP sessions that carry a full routing table (200,000+ routes) are brought up, a prolonged period of 100-percent CPU utilization (5 to 7 minutes) is experienced.

During this time, the router is unresponsive in the CLI, and it stops responding to icmp/snmp polls.

The router is a Cisco 12406/PRP and is running Cisco IOS Release 12.0(32)S5 (c12kprp-k4p-mz.120-32.S5).

When bringing up a BGP session with a full routing table, the router seems to load the first several thousand prefixes quickly and then stops dead for several minutes before loading the rest.

Workaround: After changing the outbound prefix list on the eBGP session to a deny all (ip prefix-list test-nothing-out seq 1 deny 0.0.0.0/0 le 32), clearing the BGP session does not produce the problem anymore.

- CSCsm74848

Symptoms: A crash occurs.

Conditions: All the interfaces should be up and running. To recreate the issue, perform the following steps:

- 1) Configure xconnect between PE1 and PE2.
- 2) Execute the **show xconnect all** command.
- 3) Then remove the T1 channel on which xconnect is configured.

Workaround: There is no workaround.

- CSCsm75818

Symptoms: Multicast data loss may be observed while changing the PIM mode of MDT-data groups in all core routers.

Conditions: The symptom is observed while changing the PIM mode of MDT-data groups from “Sparse” to “SSM” or “SSM” to “Sparse” in all core routers in a Multicast Virtual Private Network (MVPN).

Workaround: Use the **clear ip mroute MDT-data group** command to resolve the issue.

- CSCsm84415

Symptoms: ATM aal0-aal0 local switching fails upon SSO switchover, with L2 rewrite information missing for the corresponding VCs, resulting in traffic drops. Pseudo Wire will be down

Conditions: This symptom is observed after an SSO switchover in a scale testbed Local Switching and AToM both will be affected.

Workaround: Shutting and unshutting the involved ports resolves the issue.

- CSCsm86832

Symptoms: The line protocol of the serial interface keeps flapping.

Conditions: This symptom is observed after the Atlas BERT pattern is run on a fractional T1 (1 or 2 timeslots).

Workaround: Add/Remove the T1.

- CSCso04657

Symptoms: SSL VPN service stops accepting any new connections.

Conditions: A device configured for SSL VPN may stop accepting any new SSL VPN connections due to a vulnerability in the processing of new TCP connections for SSL VPN services. If the **debug ip tcp transactions** command is enabled and this vulnerability is triggered, debug messages with connection queue limit reached will be observed.

Workaround: There is no workaround.

- CSCso60442

Symptoms: A crash occurs.

Conditions: This symptom is observed when the **show buffers interface dump** command is entered.

Workaround: There is no workaround.

- CSCso84392

Symptoms: In MVPN, on the source PE, multicast packets are punted to the RP CPU, and some packets are also dropped.

Conditions: Ingress E3 and egress E5, and the TUNSEQ error message appears.

Workaround: There is no workaround.

- CSCso92169

Symptoms: A traceback is seen on the E3 and E5 line cards.

Conditions: This symptom is observed under normal traffic conditions after a **clear ip route *** command is issued.

Workaround: There is no workaround.

- CSCsq13938

Symptoms: In Cisco IOS software that is running the Border Gateway Protocol (BGP), the router may reload if BGP **show** commands are executed while the BGP configuration is being removed.

Conditions: This problem may happen only if the BGP **show** command is started and suspended by auto-more before the BGP-related configuration is removed, and if the BGP **show** command is continued (for example by pressing the SPACE bar) after the configuration has been removed. This bug affects BGP **show** commands related to VPNv4 address family. In each case the problem only happens if the deconfiguration removes objects that are being utilized by the **show** command. Removing unrelated BGP configuration has no effect.

This bug is specific to MPLS-VPN scenarios (CSCsj22187 fixes this issue for other address-families).

Workaround: Terminate any paused BGP **show** commands before beginning operations to remove BGP-related configuration. Pressing “q” to abort suspended show commands, rather SPACE to continue them, may avoid problems in some scenarios.

- CSCsq31233

Symptoms: The following error messages are received on a 1xoc12 eng3 line card:

```
SEC 8:May 16 06:41:09.216: %IDBINDEX_SYNC-3-IDBINDEX_ENTRY_SET: Cannot set entry to
interface index table: "", 73 -Process= "RP Standby", ipl= 0, pid= 63 -Traceback=
20A640 20A748 11D29D8 27F7A8 281F80 439B64 436AC4 5187B8 4FF360 5006FC 523434 240B7C
5C0514 5C0A14 34BC74 350B0C SEC 8:May 16 06:41:09.216: %FIB-2-HW_IF_INDEX_ILLEGAL:
Attempt to create CEF interface for Serial4/0.1/1:1 with illegal index: -1 -Traceback=
20A640 20A748 178438 17A198 17A7E8 17A980 439C1C 436ACC 5187B8 4FF360 5006FC 523434
240B7C 5C0514 5C0A14 34BC74 SEC 8:May 16 06:41:09.216: %EERP-2-UIDB_ERR: Unable to
allocate resources. Null fibhwdib for free 0
```

Conditions: This symptom is observed when either of the two tasks mentioned below is performed in the specific order and HA is configured in SSO mode.

A. Configure/Unconfigure Channels:

1. Under sonet framing, configure some T1 lines.
2. Unconfigure these T1 lines.
3. Change the framing to sdh and configure some E1 lines.
4. Unconfigure these E1 lines.
5. Change the framing to sonet and configure some T1 lines.

B. Change Framing:

1. Change the framing without deleting all the channels; a warning message to delete all channels before changing the framing will be issued.
2. Delete all the channels.
3. Change the framing multiple times from sonet to sdh, from sdh to sonet, and then from sonet to sdh again.

Workaround: There is no workaround.

- CSCsq31776

Cisco devices running affected versions of Cisco IOS Software are vulnerable to a denial of service (DoS) attack if configured for IP tunnels and Cisco Express Forwarding. Cisco has released free software updates that address this vulnerability. This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090923-tunnels.shtml>.

- CSCsq91960

Symptoms: VRF may not get deleted if the VRF NAME size is 32 characters on a dual RP HA/SSO router.

Conditions: This symptom occurs when adding a VRF with 32 characters on a DUAL RP HA router. (In some releases a VRF name with more than 32 characters will get truncated to 32.) The following may occur:

- There may be a DATA CORRUPTION ERRMSG.
- While deleting this 32 character length VRF, VRF will fail to get deleted completely with an ERRMSG on active.

Workaround: There is no workaround.

- CSCsq96435

Symptoms: Line cards get stuck in the WAITRTRY state after an RP switchover and a router reload.

Conditions: This symptom is observed on a Cisco 12810 and 12816 Internet series router that is booted with Cisco IOS Release 12.0(32)S11. The symptom is seen on both E4+ and E6 line cards and also during reload.

Workaround: There is no workaround.

- CSCsr04198

Symptoms: Traffic for certain pairs of sources and destinations is dropped.

Conditions: This symptom is observed under the following conditions:

1. Destinations are routed via a default route.
2. Load-balancing is in place.

Workaround: Break and restore load-balancing by changing IGP metrics.

- CSCsr40433

Symptoms: Traffic engineering (TE) tunnel reoptimization fails and tunnel stuck in “RSVP signaling proceeding.”

Conditions: Occurs when explicit path with loose next hops and one of the next hops is still reachable and that next hops is a dead-end.

Workaround: Use strict next hop addresses.
- CSCsr53541

Symptoms: A TE tunnel from a mesh group disappears after the tailend router is reloaded.

Conditions: The IGP is OSPF, and OSPF is used to advertise the mesh-group membership. The problem appears only if the OSPF network type is point-to-point.

Workaround: Enter the **clear mpls traffic-eng auto-tunnel mesh** command after the TE tunnel disappears from the mesh group.
- CSCsr61125

Symptoms: A switchover takes more time on a Cisco 7500 router.

Conditions: This symptom is observed when RPR+ is configured on the Cisco 7500.

Workaround: There is no workaround.
- CSCsr64777

Symptoms: A router crashes because of a block overrun (overwriting the memory block).

Conditions: This symptom is observed only when NetFlow version 5 is used.

Workaround: NetFlow version 9 could be used for exporting.
- CSCsr67137

Symptoms: An Engine 3 (E3) Channelized OC12 (CHOC12) line card can reload after a switchover in Route Processor Redundancy Plus (RPR+) mode.

Conditions: This symptom is observed on a Cisco 12416 Internet series router:
The router is booted with Cisco IOS Release 12.0(32)S11n and contains the following:

 - Redundant PRP-2 processor running in RPR+ mode.
 - E3 CHOC12 line card.
 - All other slots in the chassis are populated with E3, E4+, and E5 line cards.

Workaround: There is no workaround.
- CSCsr67289

Symptoms: Router hangs when online insertion and removal (OIR) is performed.

Conditions: Occurs after changing the interface bandwidth followed by an OIR operation.

Workaround: Stop traffic before making these changes.
- CSCsr87973

Symptoms: Linecards crash when the tunnel interface is shut down.

Conditions:

 1. The issue is seen when Tag-Switching is enabled on the VRF interface and the tunnel interface is shut down.
 2. The interface on which the tunnels are going through goes down and tunnels go down with it also.

See attachments for configuration information.

Workarounds:

1. For condition 1, the workaround is to remove the tag-switching command configured on all the affected VRF interfaces and then do a shutdown.
2. For condition 2, there is no workaround because an interface can go down when the underlying L1/L2 layer goes down.

Further Problem Description: See attachments for topology and router configurations.

- CSCsr88705

Symptoms: Redistributed routes are not being advertised after a neighbor flap.

Conditions: This symptom is observed if BGP is redistributing local routes and if there are multiple neighbors in the same update-group and then a neighbor flaps. For the flapped neighbor, some redistributed routes are not being advertised.

Workaround: Undo and redo the redistribution.

- CSCsu23084

Symptoms: The secondary RP crashes continuously.

Conditions: This symptom is observed in any Cisco IOS Release 12.0(33)S image, subject to following:

- Redundancy mode SSO.
- Several Link-bundling subinterfaces with service policies attached (Scaled Environment).
- More than 1 Engine 3 Members.

The secondary RP will crash when it is coming up, if the primary RP is already up and configured. Examples of this behavior:

- Switchover.
- The primary comes up first; the secondary is manually booted later.

Workaround: Change the redundancy mode to RPR or RPR+ to avoid the crash.

- CSCsu32015

Symptoms: A ping fails across Frame Relay subinterfaces over a non-channelized SPA.

Conditions: The ping fails across Frame Relay subinterfaces when:

- The channelized SPA is used on a bay and there are approximately 30 or more interfaces that are created and used.
- That SPA is later removed and moved to some other bay or to some other slot.
- And this current empty bay is then used for a non-channelized SPA and for Frame Relay subinterface circuits.

Workaround: There is no workaround.

- CSCsu33246

Symptoms: IPv6 PIM RP embedded functionality is not working properly in Cisco IOS Release 12.0(32)S or Release 12.0(32)SY even after the fix for CSCsf28907.

Conditions: If a first-hop router (that is connected to the IPv6 multicast source) is configured for a PIM RP embedded operation, the register packets will not be sent to the RP and the mroute table will remain in the Registering state. No IPv6 multicast traffic will flow.

Workaround: Configure an IPv6 PIM static RP.

- CSCsu36958

Symptoms: A router cannot be reloaded after the RP switches over three times.

Conditions: The router restarts three times, and each time due to watchdog timeout due to failure to allocate memory. This symptom is related to a flood of multicast messages. Once this symptom occurs, attempts to manually reload the router are unsuccessful as the NVRAM is locked, indicating that it is being updated.

Workaround: There really is no workaround except to manually remove and re-insert the RP or power-cycle the chassis.

- CSCsu40491

Symptoms: When a second multilink is enabled between a PE and a connected CPE, the route may not be propagated to the remote PE. A ping from the local PE to the CPE always works fine over both multilinks; however, a ping from the remote PE to the CPE does not work when both links are enabled.

Conditions: This symptom is observed under the following conditions:

1. The routing protocol between the PE and the CE is BGP.
2. Two static routes are defined on the PE toward the CE.
3. MLPPP is used on both links.
4. The PE is a Cisco 12000 series Internet router.
5. Both links are enabled.

These conditions do not guarantee that the problem will be reproduced; but it may occur under certain circumstances.

Workaround: Perform either of the following two workarounds:

1. To clear the issue, redefine the static routes, or shut down both multilinks and bring them back up again.
2. Enable only one multilink.

Further Problem Description: The MPLS label shows as “aggregate” instead of “untagged” during the problem.

- CSCsu41338

Symptoms: Set cos is not being applied for VPLS packets in E5 Gig. The source MAC address of the VPLS packet from the disposition PE is getting corrupted.

Conditions: This symptom is observed only for VPLS packets in E5 cards when a service policy with set cos is applied to the egress interface of the disposition PE.

Workaround: There is no workaround.

- CSCsu54160

Symptoms: An RP becomes stuck.

Conditions: This symptom is observed after an SSO mode redundancy force switchover is executed.

Workaround: Reload the secondary RP.

- CSCsu59282

Symptoms: The following message is continuously seen on SSO switchover even if the maximum scale numbers are not configured.

```
%RP-3-ENCAP: Failure to allocate encap table entry, exceeded max number of entries,
slot 3 (info 0xC0000
```

Conditions: This symptom is observed upon SSO switchover.

Workaround: Reload the RP.

- CSCsu63081

Symptoms: The **delay triggers path** *delay* command does not function as it is provisioned on an E3 CHOC12 controller.

Conditions: This symptom is observed on a Cisco 12000 Internet series router booted with c12kprp-p-mz.120-32.S11n. This router contains an E3 CHOC12 line card.

Workaround: There is no workaround.

- CSCsu65189

Symptoms: If router is configured as follows:

```
router ospf 1
...
passive-interface Loopback0
```

And is later enabled with LDP/IGP synchronization using the following commands.

```
Router(config)# router ospf 1
Router(config-router)# mpls ldp sync
Router(config-router)# ^Z
```

MPLS LDP/IGP synchronization will be allowed on the loopback interface too.

```
Router# show ip ospf mpls ldp in
```

```
Loopback0
  Process ID 1, Area 0
  LDP is not configured through LDP autoconfig
  LDP-IGP Synchronization : Required < ---- NOK
  Holddown timer is not configured
  Interface is up
```

If the **clear ip ospf proc** command is entered, LDP will keep the interface down. Down interface is not included in the router LSA, therefore IP address configured on loopback is not propagated. If some application like BGP or LDP use the loopback IP address for the communication, application will go down too.

Conditions: Occurs when interface configured as passive. Note: all interface types configured as passive are affected, not only loopbacks.

Workaround: Do not configure passive loopback under OSPF. The problem occurs only during reconfiguration.

The problem will not occur if LDP/IGP sync is already in place and:

- The router is reloaded with image with fix for CSCsk48227.
- The **passive-interface** command is removed/added.

- CSCsu66119

Symptoms: If “set exp” is configured on the ingress AC, local switching (AC - AC) traffic does not copy the exp value to the cos bits in the egress direction.

Conditions: This symptom is observed with E3 as ingress and “set exp” configured on VPLS interface.

Workaround: There is no workaround.

- CSCsu73675

Symptoms: In the case of E5 AToM QinQ, set cos is being set on the inner vlan_id.

Conditions: This symptom is observed in an E5 AToM with QinQ configuration that has set cos in the policy map.

Workaround: There is no workaround.

- CSCsu74140

Symptoms: In E5 L2TPv3 dot1q set cos is not setting on the vlan-id.

Conditions: This symptom is observed in a configuration that has set cos in the policy.

Workaround: There is no workaround.

- CSCsu79988

Symptoms: Before this BGP aspath memory optimization, the memory consumption for aspath has increased. With this memory optimization, the memory consumption for aspath is reduced.

Workaround: There is no workaround.

- CSCsu84357

Symptoms: The **show mac address-table bridge-domain domain** command may display unexpected MAC addresses.

Conditions: This symptom has been reported on a Cisco 12000 series Internet router that is configured with VPLS. When a service policy with input policing is applied on an interface that also has bridge-domain configured and when police drops happen, ghost MAC addresses are present in the MAC address table for that bridge-domain ID.

Workaround: There is no workaround. But no immediate impact on system behavior has been observed.

Further Problem Description: This issue can occur with either ACL drops or policer drops on a VPLS-enabled interface. If there are no ACL or CAR drops, this issue will not occur.

This unexpected MAC address might conflict with another real MAC address and may lead to some other issues such as traffic being sent over the wrong interface for the same customer.

Let us assume that the customer is having two ACs on the same PE and that AC1 learned the proper MAC address and the unexpected MAC address. If this unexpected MAC address is a valid MAC address on AC2, then the traffic for this MAC address may be sent to AC1 instead of to AC2.

- CSCsu86288

Symptoms: A line card on a Cisco 12000 series Internet router generates tracebacks during LI provisioning while installing a 50th tap request. After the appearance of the first traceback, LI functionality stops working for newly requested taps.

Conditions: This symptom is observed when there are 48 active taps and 2 new taps arrive.

Workaround: Reload the line card or the whole router.

- CSCsu89509

Symptoms: When PEM PS is inserted, there is an increase in CPU utilization by the PowerMgr Main process. The utilization is from 10 percent to 99 percent; the difference is caused by inserting timing.

Conditions: This issue is observed under the following conditions:

- 16-slot chassis
- Enhanced fabric
- Enhanced CSC

- DC PEM

Workaround: There is no workaround.

- CSCsu92317

Symptoms: Pings fail on an MLPPP interface.

Conditions: There is an MFR interface used for L2 services such as xconnect and an MLPPP interface on the same SPA. When the member links are removed/added from these bundles back-to-back, the ping on the MLPPP interface may fail. This symptom is observed so far only on E5 cards.

Workaround: Reload the line card.

- CSCsu93472

Symptoms: Whenever a service policy that has an action as bandwidth or shaping is applied as output to the core-facing interface in an imposition PE in a VPLS setup, the egress multicast packets that are passing through the core-facing interface are being dropped.

Conditions: This symptom is observed when:

- A service policy with action as bandwidth or shaping is applied as output to the core-facing interface in an imposition PE in a VPLS setup; and
- Multicast traffic is flowing through the interface.

Workaround:

- 1) Remove and re-add the bridge-domain.
- 2) Reload the ingress line card that has bridge-domain configured on it.

- CSCsu93501

Symptoms: In Cisco IOS Release 12.0(33)S, the VPLS-specific ingress policy matches are not working for the multicast and VPLS-unknown classes. Either class will match all unicast, multicast, broadcast, and unknown traffic.

Conditions: This symptom is observed for multicast and VPLS-unknown traffic that passes through the VPLS-specific ingress policy in Cisco IOS Release 12.0 (33)S images only.

Workaround: There is no workaround.

- CSCsv00039

Symptoms: A customer observed the following message in the log:

The PAM_PIM created confusion as it was being referred to Protocol Independent Multicast and not to the Packet Assembly Module/Packet Interface Module.

Conditions: This symptom occurs because of a corrupted packet.

Workaround: There is no workaround.

- CSCsv04674

Symptoms: The M(andatory)-Bit is not set in Random Vector AVP, which is a must according to RFC2661.

Conditions: This symptom is observed with Egress ICCN packet with Random Vector AVP during session establishment.

Workaround: There is no workaround.

- CSCsv04836

Multiple Cisco products are affected by denial of service (DoS) vulnerabilities that manipulate the state of Transmission Control Protocol (TCP) connections. By manipulating the state of a TCP connection, an attacker could force the TCP connection to remain in a long-lived state, possibly indefinitely. If enough TCP connections are forced into a long-lived or indefinite state, resources on a system under attack may be consumed, preventing new TCP connections from being accepted. In some cases, a system reboot may be necessary to recover normal system operation. To exploit these vulnerabilities, an attacker must be able to complete a TCP three-way handshake with a vulnerable system.

In addition to these vulnerabilities, Cisco Nexus 5000 devices contain a TCP DoS vulnerability that may result in a system crash. This additional vulnerability was found as a result of testing the TCP state manipulation vulnerabilities.

Cisco has released free software updates for download from the Cisco website that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090908-tcp24.shtml>.

- CSCsv08408

Symptoms: A router may crash due to a bus error due to an illegal access to a low address because IPC is processing a message that is already returned back to the pool, but still the message's reference is present in IPC's retry table.

Conditions: The conditions under which this symptom occurs are not known.

Workaround: There is no workaround.

- CSCsv15604

Symptoms: E4+ on a Cisco 12000 series Internet router stops exporting NetFlow. Show commands display that packets are correctly captured and exported.

Conditions: Traffic should flow through an E4+ and go out through an E5, which has to be MPLS enabled.

Workaround:

- 1) Change the outbound interface configuration to IP.
- 2) Add a static route for the NFC using the non-recursive next hop.

- CSCsv16911

Symptoms: I have created a few flow monitors, and I tried to add the flow monitors in one direction on which IPHC was configured and it gave a linecard failure message; when I tried the same procedure a second time, it was added.

Conditions: All the serial interfaces should be up and running.

Workaround: There is no workaround.

- CSCsv18049

Symptoms: Presently we do not support processing multiple filter specs in the Resv Error message. We process only the first filter spec in the list. Not processing the other LSPs in the RESVError will lead to inconsistent states.

Conditions: This symptom is observed on a Cisco 12000 series Internet router that has a PRP-2 and that is running Cisco IOS Release 12.0(32)SY6.

Workaround: There is no workaround.

- CSCsv23328

Symptoms: Default Q-limit is not getting doubled for low-speed interfaces.

1) Non-channelized SPA

2) For policy without queueing action on non-channelized SPA

Conditions: Default Q-limit for low-speed interfaces should be doubled as required.

This should be done only for low-speed interfaces. Rates that will get 64K queue-limit and above. I.e., starting from 32K, the queue-limits will not get doubled.

For example, 64K in will be trimmed to 32K from this release onward and likewise for further queue-limits. Also, it is taken care that the class rate ranges 2097152 - above will get max_queue_depth of 256K as they always got.

For more info, please also refer to DDTS CSCsu60240.

Workaround: Reload the SPA.

- CSCsv25593

Symptoms: If the BFD session count exceeds the limits, an error message is printed within the debug flag.

Conditions: The linecard supports 100 sessions, and the chassis supports 200 sessions in Cisco IOS Release 12.0(33)s throttle only.

Workaround: If the BFD session count exceeds the limits, remove and add the BFD from the interface.

- CSCsv26606

Symptoms: A 1xCHOC12 controller goes down, and all links flap.

Conditions: This symptom is observed when the **show plim datapath details** command is executed on the line card, which dumps a lot of information on the console.

Workaround: Avoid using the **show plim datapath details** command; instead, use the per-channel **show plim datapath channel-id details** command.

- CSCsv27470

Symptoms: An Engine 3 CHOC12 fails to bring the T1 controller link down when the **delay triggers path** command is configured.

Conditions: Shutting down the remote end T1 controller or CHOC12 T1 controller receive AIS will not cause the T1 link to go to down state.

Workaround: Do not configure the **delay triggers path** command on the CHOC12 SONET controller.

- CSCsv27607

Symptoms: BGP router filters outbound routes to the peers when doing soft reset with specifying peer address using the **clear ip bgp ip-address soft out** command. However, the routes to be filtered are not deleted from the routing table on the BGP peer router.

Conditions: The symptom happens when removing and then reapplying an outbound route-map. When issuing the **clear ip bgp neighbor-address soft out** command for each peer in an update-group after applying the outbound route-map filtering policy. The withdraw for filtered prefixes is sent to the first peer specified in soft reset, but the next peers in the same update-group do not withdraw the routes.

Workaround: Perform a hard BGP reset using the **clear ip bgp ip-address** command.

- CSCsv38557

Symptoms: POS interfaces run into a tx stuck condition, and heavy packet drops occur in the local switching path. The VIP CPU runs high due to the Rx- Side Buffering mechanism that kick starts in the local switching path in the VIP.

Conditions: This symptom is observed on a Cisco 7500 node with a VIP that has the POS interfaces up and data traffic being locally switched between the POS interfaces. This symptoms is triggered when a service policy is applied/removed followed by interface flaps.

Workaround: “test rsp stall” cleans up the Rx-Side buffered packets. Hence this could be considered a workaround. However, this does not always help. Doing a soft OIR removal and insertion of the LC always helps recover from this situation. The best workaround is to apply a service policy.

- CSCsv57665

Symptoms: A router is not learning MAC addresses when unknown multicast traffic (packet size greater than min_mtu for that VFI towards core) is sent.

Conditions: This symptom is observed when the MTU of the core-facing interface is changed to some value less than the default value and then is increased back to the default. The min_mtu is stuck on the lesser value.

Workaround: There is no workaround.

- CSCsv66827

Symptoms: Clearing the SSH sessions from a VTY session may cause the router to crash.

Conditions: The symptom is observed when a Cisco 7300 series router is configured for SSH and then an SSH session is connected. If the SSH session is cleared every two seconds using a script, the symptom is observed.

Workaround: There is no workaround.

- CSCsv73509

Symptoms: When “no aaa new-model” is configured, authentication happens through the local even when tacacs is configured. This happens for the exec users under vty configuration.

Conditions: Configure “no aaa new-model,” configure login local under line vty 0 4, and configure login tacacs under line vty 0 4.

Workaround: There is no workaround.

- CSCsv74508

Symptom: If a linecard is reset (either due to error or a command such as hw-module slot reload) at the precise time an SNMP query is trying to communicate with that LC, the RP could reset due to a CPU vector 400 error.

Conditions: In order to experience these symptoms the linecard is reset (either due to error or a command such as hw-module slot reload) at the precise time an SNMP query is received.

Workaround: There is no workaround.

- CSCsv82120

Symptoms: A CHOC12 T1 continuously flaps when the T1 link that is connected to a third-party CE router flaps. With the Cisco router, the same issue is not observed.

Conditions: This symptom is observed under the following conditions:

- Cisco IOS Release 12.0(32)S11n
- CHOC12 T1 links with a third-party CE router

Workaround: Disable “yellow detection” on the CHOC12 T1 link. For example, serial interface 12/0.7/6:0:

```
controller sonet 12/0
sts-1 7
no t1 6 yellow detection
! Wait for the T1 to stabilize.
t1 6 yellow detection
```

- CSCsv84690

Symptoms: The source MAC address is not learned properly for the bridge domain associated with a VFI instance.

Conditions: Traffic is from CE2-----PE1-----CE1 (locally switched). Source MAC addresses of packets from CE2 are not learned correctly. NetFlow is enabled on the interfaces of the PE.

Workaround: Disable NetFlow on the main interface.

- CSCsv94306

Symptoms: On a Cisco 12000 series Internet router E5/SPA POS interface, FRR reroute may take up to 700 msec.

Conditions: This symptom is observed when the far-end RX fiber of the POS link is removed.

Workaround: Configure the **pos delay triggers** command on the interface to reduce delay in FRR.

Further Problem Description: When the RX fiber is removed on the far-end of the POS interface, the far-end router is supposed to send LRDI to the Cisco 12000 series Internet router, and the LRDI will trigger the FRR reroute. The E5/SPA current implementation is that remote end SONET alarm does not trigger FRR in interrupt mode; it triggers FRR only in process context, which may take up to 700 msec to converge.

- CSCsv96395

Symptoms: A SIP-400 and SIP-601 crash continuously after the image is loaded.

Conditions: After the 32SY 11_23-date-coded image is loaded, SIP crashes when channelized SPAs come up.

Workaround: There is no workaround.

- CSCsw17389

Symptoms: A SPA_PLIM-3-HEARTBEAT failure and tracebacks are seen for channelized SPAs. All the traffic in the ingress direction is dropped.

Conditions: With traffic present, configure aggregate NF scheme on 4XT3/E3 SPA; channelized SPAs get stuck in the booting state. (SIP comes up fine to IOS RUN state.)

Workaround: Perform a microcode reload to make the SPAs come up.

- CSCsw17390

Symptoms: A PVC flaps with the following error message:

```
ATM(ATM3/0/0.504): VC(17) Bad SAP received 00AD
```

Conditions: This symptom is observed on a Cisco 7600 with a FlexWAN and PAA3 when connected to a Cisco 12000 ATM interface and when the PVC is configured for bridging.

Workaround: There is no workaround.

- CSCsw19951

Symptoms: A SUP720 may reset with the following:

```
RP: %C6K_PLATFORM-2-PEER_RESET: RP is being reset by the SP
```



```

SP or DFC: Address Error (load or instruction fetch) exception, CPU signal 10, PC =
0x40B0D738 -Traceback= XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX $0 : XXXXXXXX, AT
: XXXXXXXX, v0 : XXXXXXXX, v1 : XXXXXXXX a0 : XXXXXXXX, a1 : XXXXXXXX, a2 : XXXXXXXX,
a3 : XXXXXXXX t0 : XXXXXXXX, t1 : XXXXXXXX, t2 : XXXXXXXX, t3 : XXXXXXXX t4 : XXXXXXXX,
t5 : XXXXXXXX, t6 : XXXXXXXX, t7 : XXXXXXXX s0 : XXXXXXXX, s1 : XXXXXXXX, s2 :
XXXXXXXX, s3 : XXXXXXXX s4 : XXXXXXXX, s5 : XXXXXXXX, s6 : XXXXXXXX, s7 : XXXXXXXX t8
: XXXXXXXX, t9 : XXXXXXXX, k0 : XXXXXXXX, k1 : XXXXXXXX gp : XXXXXXXX, sp : XXXXXXXX,
s8 : XXXXXXXX, ra : XXXXXXXX EPC : XXXXXXXX, ErrorEPC : XXXXXXXX, SREG : XXXXXXXX MDL0
: XXXXXXXX, MDHI : XXXXXXXX, BadVaddr : XXXXXXXX DATA_START : 0XXXXXXXX Cause
XXXXXXXX (Code 0xX): Address Error (load or instruction fetch) exception

```

Conditions: This symptom is observed on a device that is configured with MPLS.

Workaround: There is no workaround.

- CSCsw24700

Cisco IOS software contains two vulnerabilities within the Cisco IOS WebVPN or Cisco IOS SSLVPN feature (SSLVPN) that can be remotely exploited without authentication to cause a denial of service condition. Both vulnerabilities affect both Cisco IOS WebVPN and Cisco IOS SSLVPN features:

1. Crafted HTTPS packet will crash device - Cisco Bug ID CSCsk62253.
2. SSLVPN sessions cause a memory leak in the device - Cisco Bug ID CSCsw24700.

Cisco has released free software updates that address these vulnerabilities.

There are no workarounds that mitigate these vulnerabilities.

This advisory is posted at the following link:

<http://www.cisco.com/warp/public/707/cisco-sa-20090325-webvpn.shtml>

- CSCsw30847

Symptoms: The standby router may crash.

Conditions: The symptom is observed when two IMA interfaces are configured on a Cisco 7500 series router along with HA RPR+ mode. When you try to unconfigure the ima-group from the first member of IMA interfaces, the crash will occur.

Workaround: There is no workaround.

- CSCsw31009

Symptoms: CEF Scanner takes high CPU for sustained periods of time around 10 minutes.

Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.0(32)S11n. It is seen under the following conditions:

- When multiple eiBGP paths exist for a certain prefix and the eBGP path is recursive through the attached next-hop.
- A large number of prefixes that have one iBGP path that is recursive through an IGP route that has one path, and one iBGP path that is recursive through an IGP route that has multiple paths.
- A route modification for load-balanced prefix.

Workaround: Configure a static route.

- CSCsw34455

Symptoms: After a reboot, GEs remain down/down on a SPA-10X1GE-V2.

Conditions: This symptom is observed on a Cisco 12000 series Internet router that is using a 12000-SIP-601 with a SPA-10X1GE-V2 and Cisco IOS Release 12.0 (32)SY6.

Workaround: Shut and unshut the port that is down/down.

- CSCsw35638

Symptoms: When a Cisco router is the Merge Point (MP) for a protected TE tunnel, and FRR is triggered, two things happen:

- The primary LSP goes down, and traffic is lost on the protected tunnel.
- Any PLR that is downstream of the failure will lose its backup.

Conditions: When a competitor's router is a point of local repair (PLR) and a Cisco router is a merge point, then when FRR is triggered, the Cisco router drops the backup tunnel (in some cases immediately and in other cases after 3 minutes). This causes the primary tunnel that is protected by this backup to go down. The issue has been identified as related to the fact that session attribute flags (link/node protection desired) are being cleared by the competitor PLR when the Path is sent over the backup tunnel.

Workaround: There is no workaround.

- CSCsw47346

Symptoms: A switchover cannot be performed on a Cisco 7500 router.

Conditions: This symptom is observed when test crash is issued on a VIP console.

Workaround: There is no workaround.

- CSCsw47868

Symptoms: An IPv6 ping fails on an E3 Gigabit line card because of a PRECAM 1 Exception.

Conditions: This issue pertains to the dropping of IPv6 packets because of a precam exception on the egress side. It looked as if the profile for IPv6 was wrong when IPv4 QoS was already applied even on different subinterfaces on the same port.

Workaround:

- 1) Add/Remove an ACL.
- 2) Add/Remove the subinterface.

- CSCsw51017

Symptoms: In the case of egress MVPN QoS, some packets are going to the wrong queue.

Conditions: This symptom is observed with an egress MVPN QoS configuration.

Workaround: There is no workaround.

- CSCsw64956

Symptoms: The **no ppp lcp fast-start** command is added to all PPP-encapsulation interfaces.

Conditions: This symptom is observed after a router is upgraded from Cisco IOS Release 12.0(32)SY7 to the latest 32sy throttle image.

Workaround: There is no workaround.

- CSCsw69322

Symptoms: Given the following topology:

PE1 (CT32/2/1) <-----> (CT34/0/1) CE1

Configuring t1 <1-28> loopback remote line feac at PE1 and then removing the loopback causes the serial interface at CE1 to start flapping continuously.

Conditions: All the interfaces should be up and running.

Workaround: There is no workaround.

- CSCsw74258
Symptoms: An Engine 5 linecard crashes.
Conditions: This symptom is observed when MLPPP member links are swapped from one MLPPP bundle to another MLPPP bundle.
Workaround: There is no workaround.
- CSCsw79733
Symptoms: RTP timestamp is getting corrupted with a sequence of RTP packets.
Conditions: Conditions are FH/cRTP/cUDP/cRTP. cUDP is sent if there is some change in RTP header like the Marker bit is set, the payload type changes, the CSRC list is there. This symptom is seen only with the IPHC compression format.
Workaround: Configure the IETF compression format.
- CSCsw80606
Symptoms: A router crashes.
Conditions: This symptom is observed when the **copy scp: disk0:** command is issued to transfer the file to disk0: of the router.
Workaround: There is no workaround.
- CSCsw82329
Symptoms: A SIP-601 crashes continuously. The line card (LC) stops crashing when the SPA-1XCHSTM1/OC3 SPA is shut. The LC does not stop crashing with any other exercise like LC OIR, SPA OIR, or router reload.
Conditions: This symptom was observed while the router was being brought up. The router was initially shut and was later powered up.
Workaround: Shut the SPA to cause the LC to stop crashing.
- CSCsw90192
Symptoms: A CT3 controller on a CH OC3 SPA remains down after a SPA reload.
Conditions: SPA reload.
Workaround: Enable and disable the BITS feature to clear the issue.
- CSCsw90592
Symptoms: Traffic does not flow for some VCs through the SR-APS interface.
Conditions: This symptom is observed after a LC reload and a router reload.
Workaround: Shut/no shut of SR-APS interface.
- CSCsw93321
Symptoms: If the Flexible NetFlow feature is used on a Cisco 12000 series Internet router along with sampled NetFlow, packets are dropped through the router. The packet drop rate is equal to the configured sampler rate.
Conditions: This symptom has been reported on a Cisco 12000 series Internet router that is running Cisco IOS Release 12.0(33)S1. The symptom is triggered only if both Flexible NetFlow *and* sampled NetFlow are used together on same interface.
Workaround: There is no workaround.

- CSCsx08901

Symptoms: The following message is received from the standby RP:

```
SEC 8:Jan 13 23:11:09.991: SPA CHOCX ALARM MSG:
spa_chocx_update_sonet_ctrlr_alarm_status : mib is NULL plugin = 0xA7357E4 line_id =
0 SEC 8:Jan 13 23:11:09.991: -Traceback= 20E8FC 929F50 929E1C 929D64 928B58 928A98
9335D8 4FAA38 4C09E0 362A84 35EED8 35EF30 2F92DC Jan 13 23:11:10.987 UTC:
%SONET-4-ALARM: SONET 14/2/0: SLOS Jan 13 23:11:10.987 UTC: %CONTROLLER-5-UPDOWN:
Controller SONET 14/2/0, changed state to down SEC 8:Jan 13 23:11:10.991:
spa_chocx_update_sonet_ctrlr_alarm_status : mib is NULL plugin = 0xA7357E4 line_id =
0 SEC 8:Jan 13 23:11:10.991: -Traceback= 20E8FC 929F50 929E1C 929D64 928B58 928A98
9335D8 4FAA38 4C09E0 362A84 35EED8 35EF30 2F92DC
```

Conditions: This symptom is observed after the framing on the chstm1 SPA card is changed.

Workaround: There is no workaround.

- CSCsx10140

Recent research (1) has shown that it is possible to cause BGP sessions to remotely reset by injecting invalid data, specifically AS_CONFED_SEQUENCE data, into the AS4_PATH attribute provided to store 4-byte ASN paths. Since AS4_PATH is an optional transitive attribute, the invalid data will be transited through many intermediate ASes which will not examine the content. For this bug to be triggered, an operator does not have to be actively using 4-byte AS support.

The root cause of this problem is the Cisco implementation of RFC 4893 (4-byte ASN support) - this RFC states that AS_CONFED_SEQUENCE data in the AS4_PATH attribute is invalid. However, it does not explicitly state what to do if such invalid data is received, so the Cisco implementation of this RFC sends a BGP NOTIFICATION message to the peer and the BGP session is terminated.

RFC 4893 is in the process of getting updated to avoid this problem, and the fix for this bug implements the proposed change. The proposed change is as follows:

“To prevent the possible propagation of confederation path segments outside of a confederation, the path segment types AS_CONFED_SEQUENCE and AS_CONFED_SET [RFC5065] are declared invalid for the AS4_PATH attribute. A NEW BGP speaker MUST NOT send these path segment types in the AS4_PATH attribute of an UPDATE message. A NEW BGP speaker that receives these path segment types in the AS4_PATH attribute of an UPDATE message MUST discard these path segments, adjust the relevant attribute fields accordingly, and continue processing the UPDATE message.”

The only affected version of Cisco IOS software that supports RFC 4893 is Cisco IOS Release 12.0(32)S12, released in December 2008.

(1) For more information please visit:

<http://www.merit.edu/mail.archives/nanog/msg14345.html>

- CSCsx23456

Symptoms: The standby reloads on a Cisco 7500 series router.

Conditions: The symptom is observed when IMA PA is configured on a Cisco 7500 series router and where RPR+ is configured. It is seen when an OIR is done on the VIP where IMA PA is sitting.

Workaround: There is no workaround.

- CSCsx23559

Symptoms: With a nested policy map, when EF traffic is sent at police rate or above police rate, BFD flaps. The BFD timer is set to 999 ms*3, while the EF traffic average latency is only 50 to 70 microseconds.

Conditions: This symptom is observed when a nested policy is applied to ocpos3 and cht3 SPA with FR encapsulation.

Workaround: There is no workaround.

- CSCsx25461

Symptoms: With a Cisco IOS Release 12.0(32)SY image, BGP I/O spikes CPU up to 9 percent because of a BGP neighbor flap with a single BGP neighbor. When multiple eBGP neighbors flap at the same time, the BGP I/O can sometimes spike up to approximately 20 percent.

Conditions:

bgp neighbor reset

Workaround: There is no workaround.

- CSCsx29281

Symptoms: Packets get corrupted along the path. Extra padding is added to the packets, and the packets become unusable by the receiver application.

Conditions: Frame Relay VPWS between Cisco 12000 series Internet router's with small 25-byte non-IP packets.

Workaround: There is no workaround.

- CSCsx31693

Symptoms: All L2VPN traffic is dropped for more than 1 minute around 20 to 30 seconds after another linecard is reinserted.

Conditions:

- ToFab QoS is configured (rx-slot-cos commands).
- L2VPN (both AToM and VPLS) traffic on E5 is affected.
- Cisco IOS Release 12.0(32)SY7.
- 900 VCs are configured.

Workaround: Remove the rx-slot-cos part of the configuration.

- CSCsx32416

Symptoms: A session may go down one or more times before stabilizing in the up state.

Conditions: This symptom is observed when a BFD session is first coming up and the network is suffering from congestion.

Workaround: There is no workaround.

- CSCsx42179

Symptoms: In MPLS VPN each tunnel is associated with one or more virtual routing and forwarding (VRF) instances. A VRF defines the VPN membership of a customer site attached to a PE router. Traffic entering a network on a non-VRF interface may be incorrectly forwarded to a VRF.

Note: Traffic from a VRF to another private or a public network is not incorrectly routed.

Conditions: This issue is only experienced in Cisco 12000 Series Internet Routers running Cisco IOS Releases 12.0(32)S and 12.0(32)SY. Additionally, the affected device must have NetFlow enabled and configured with an Engine 3 Line Card (LC).

This issue is only experienced in very rare conditions where routing table fluctuations take place as the result of route flapping.

Workaround: Create a default IP route destined to null 0 in the global routing table, as demonstrated in the following example:

```
ip route 0.0.0.0 0.0.0.0 null 0
```

- CSCsx46184

Symptoms: In case of E5 FRoMPLS, small-sized frames that are less than 34 bytes are getting corrupted because of the padding that is being added. Traffic is not getting dropped as the L2 header (DLCI) is intact; only the extra padding that gets added to the payload is being dropped.

Conditions: This symptom is observed when E5 is acting as edge for FRoMPLS.

Workaround: There is no workaround.

- CSCsx55779

Symptoms: A SIP-601 is reset after local switching is configured. After the linecard comes up, traffic does not flow end to end on the local switching attachment circuit.

The issue is seen only when the Frame Relay frame size is less than 12 bytes (4 bytes FR header + 4 bytes FCS + 0-4 bytes payload) and when the NLPID value is 0x00 (that is, an invalid Frame Relay encapsulation). From RFC 2427:

An NLPID value of 0x00 is defined within ISO/IEC TR 9577 as the Null Network Layer or Inactive Set. Because it cannot be distinguished from a pad field, and because it has no significance within the context of this encapsulation scheme, an NLPID value of 0x00 is invalid under the Frame Relay encapsulation.

Conditions: Traffic should be enabled while doing local switching configurations.

Workaround: There is no easy workaround. Shut down the interface before the hw-module reload of the linecard.

- CSCsx69785

Symptoms: 8-port OC48 E6 linecards crash when trying to bring up back-to-back connected or looped back (between two OC48 interfaces on the same E6 linecard) interfaces. This can also be seen when the optic cable/SFP is removed and inserted continuously between the back-to-back or loopback OC48 interfaces on the E6 linecard.

Conditions: On back-to-back connected or loopback (through two ports on the same linecard) connected E6 OC48 ports, performing a shut/no shut crashes the E6 linecards. Also, removing and inserting the optic cable/SFP repeatedly in the back-to-back or loopback connection (which is in the “no shut” state) between two OC48 ports on E6 cards crashes the E6 linecard.

Workaround: Configure clock source internal before configuring no shut.

- CSCsx81775

Symptoms: An Engine 5 line card (SIP-x01) crashes when a QoS configuration is applied to a serial interface.

Conditions: This symptom is observed when applying a service policy to a serial interface with several classes with a Police + WRED configuration, with more than two of the following:

1. Class-default with WRED+Police action.
2. One or more classes matching on prec/dscp with WRED+Police action.
3. One or more classes matching on Access-group with WRED+Police action.
4. Any class with a “Match Any” condition with WRED+Police.

Workaround: There is no workaround. Such a policy is not supported.

- CSCsx90461
Symptoms: A SIP 601 crashes in a PE router mvpn scenario.
Conditions: This symptom is observed while flapping core-facing or edge-facing interface.
Workaround: There is no workaround.
- CSCsy03689
Symptoms: The IP address of one of the SDCC interfaces is not seen.
Conditions: This symptom is observed after the router is reloaded.
Workaround: There is no workaround.
- CSCsy06379
Symptoms: In reloading the E5 with CT3, it resets three to four times, and also the core-facing E5 with 10x1GE crashes a couple of times before stabilizing.
Conditions: This symptom is observed in a scale testbed that is running an MVPN profile.
Workaround: Stop the traffic until the linecard comes up and then start the traffic.
- CSCsy09839
Symptoms: QoS class of service queues are in an unallocated state on the standby RP of a router that is configured in SSO mode upon router reload.
Conditions: The following conditions should exist to hit this DDTs:
 - A Cisco 12000 series Internet router with E3 LC configured in SSO mode.
 - Scale number of output service policy configured on the interfaces of E3 LC.
 - Reload of router configured in SSO mode.Workarounds:
 - 1) Reload the E3 LC after the router configured in SSO mode has come up.
 - 2) Remove and add the affected service policies on E3 LC.
- CSCsy20021
Symptoms: Ping and traffic drops occur on LB local switching circuits.
Conditions: This symptom is observed when an RPR+ switchover is performed.
Workaround: There is no workaround.
- CSCsy29345
Symptoms: An E3 1*CHOC12 LC_ENABLED is not sent to the standby RP in SSO mode.
Conditions: This symptom is observed when a router that is configured in SSO mode is reloaded.
Workaround: There is no workaround.
- CSCsy33936
Symptoms: The CEF process is hogging the CPU because of many incomplete fibidbs, because CEF was disabled and re-enabled.
Conditions: This symptom is observed in a scale testbed when an RPR+ switchover is performed.
Workaround: There is no workaround.
- CSCsy57746
Symptoms: The standby PRP2 crashes many times during a reload.

Conditions: The problem occurs only during the boot-up process. The router:

- Should have two processors (in this case PRP2) that are running SSO as the redundancy mode.
- Should be running Cisco IOS Release 12.0(32)SY6e.
- Should have a high scale (so a large configuration).
- Should have many MLPPP interfaces.

Workaround: There is no workaround.

Further Problem Description: The standby processor crashes many times during boot-up when the router has a high scale (a large configuration) and many MLPPP interfaces.

The problem happens on a Cisco 12000 series Internet router with two PRP2s that are working in SSO mode and that are running Cisco IOS Release 12.0(32) SY6e.

After the reload, exactly when MLPPP is coming up (establishing), the Cisco 12000 series Internet router suffers high CPU utilization and it loses communication with the standby router for some seconds. When the timeout occurs (when the time expires), the router requests the standby PRP to reset.

- CSCsy66775

Symptoms: PPLB drops some packets upon loadsharing with an odd number of links.

Conditions: This symptom is observed when there is an odd number of interfaces for load balancing.

Workaround: There is no workaround.

- CSCsy81103

Symptoms: An E5 crashes when the **show contr rewrite** command is executed.

Conditions: This symptom is observed on a Cisco 12000 series Internet router that is configured with LB.

Workaround: There is no workaround.

- CSCsy98079

Symptoms: Although ATOM VCs are up, pings are not working between CE routers, and tracebacks are also observed.

Conditions: When L2TPv3 is used with ATOM, connectivity breaks between CE routers.

Workaround: There is no workaround.

- CSCsz01358

Symptom: A linecard crashes continuously when a microcode reload is performed.

Conditions: The interfaces of the crashing linecard are part of port-channel, and traffic is flowing via that linecard.

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.0(33)S2

All the caveats listed in this section are resolved in Cisco IOS Release 12.0(33)S2. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCeb54456

Symptoms: A Data-link switching plus (DLSw+) circuit may not function when a TCP connection gets stuck. After about 90 seconds, the TCP connection is closed by DLSw+, and a new TCP connection is built for DLSw+. Once the new TCP connection is up, the DLSw+ circuit starts functioning again.

Conditions: This symptom is observed on a Cisco router that is configured with both a DLSw+ interface and an ATM interface.

Possible Workaround: If this is an option, remove the ATM interface from the router. When you configure the DLSw+ interface and the ATM interface on different routers, the symptom does not occur.

- CSCek79311

Symptoms: Under stress conditions, an L2TP multihop node may crash.

Conditions: This symptom is observed when a session is being disconnected.

Workaround: There is no workaround.

- CSCse05292

Symptoms: A static map configuration for an ATM PVC that uses the **protocol ip ip-address** command is rejected, giving an ambiguous command error.

Conditions: This symptom is observed when you configure a static map on an ATM PVC using the **protocol ip ip-address** command.

Workaround: Explicitly configure the [**broadcast | no broadcast**] option:

```
Router(config-if-atm-vc)# protocol ip 10.10.100.2 broadcast
Router(config-if-atm-vc)# protocol ip 10.10.100.2 ?
broadcast Pseudo-broadcast
no Prevent Pseudo-broadcast on this connection
<cr>
Router(config-if-atm-vc)# protocol ip 10.10.100.2 no broadcast
Router(config-if-atm-vc)#
```

- CSCsi68795

Symptoms: A PE that is part of a confederation and that has received a VPNv4 prefix from an internal and an external confederation peer, may assign a local label to the prefix despite the fact that the prefix is not local to this PE and that the PE is not changing the BGP next-hop.

Conditions: The symptoms are observed when receiving the prefix via two paths from confederation peers.

Workaround: There is no workaround.

Further Problem Description: Whether or not the PE will chose to allocate a local label depends on the order that the multiple paths for this VPNv4 prefix are learned. The immediate impact is that the local label allocated takes up memory in the router as the router will populate the LFIB with the labels.

- CSCsi77983

Symptoms: The NetFlow cache runs out of space for new flow entry when customer uses heavy traffic.

Conditions: Large amount of traffic, which could exhaust the NetFlow cache.

Workaround: There is no workaround.

- CSCsj30417

Symptoms: In Eng3 ATM, when a subinterface flaps, traffic to certain destinations is forwarded to the wrong subinterface.

Conditions: This symptom is observed in Cisco IOS Release 12.0(32)S05 and 12.0(32)S06. The symptom is not found in Cisco IOS Release 12.0(31)S2.

Workaround: There is no workaround; however, reloading the line card solves the problem.

- CSCsj36133

Symptoms: A BGP neighbor may send a notification reporting that it received an invalid BGP message with a length of 4097 or 4098 bytes.

Conditions: The problem can be seen for pure IPv4 BGP sessions (no MP-BGP in use) when the router that is running the affected software generates a large number of withdraws in a short time period and fills an entire BGP update message (up to 4096 bytes normally) completely with withdraws. Because of a counting error, the router that is running the affected software can generate an update message that is 1 or 2 bytes too large when formatting withdraws close to the 4096 size boundary.

Workaround: The issue is not seen when multiple address families are being exchanged between BGP neighbors.

- CSCsj49293

Symptoms: The interface output rate (214 Mb/s) is greater than the interface line rate (155 Mb/s).

Conditions: This symptom is observed with a Cisco 7600/7500/7200-NPE400 and below. That is, PA-POS-2OC3/1OC3 (PULL mode).

Workaround: There is no workaround.

Further Problem Description: From the Ixia, packets are transmitted at 320 Mb/s. On the UUT (Cisco 7600), the outgoing interface (POS-Enhanced Flexwan) shows the output rate as 200 Mb/s. But the interface bandwidth is 155 Mb/s.

- CSCsk68742

Symptoms: The **show ip mds stats linecard** command shows MDFS reloads on all line cards.

Conditions: This symptom is observed when multicast distributed routing is added on a VRF through the configuration of the **ip multicast-routing vrf vpn distributed** command.

Further Problem Description: Note that while the MDFS reload is a real reload, it is without a preceding clear, so it will not generally cause traffic interruption because it merely causes the same information to be downloaded to the line cards again. However, in a highly scaled system that is running close to the limit, the additional load introduced by a full MDFS reload of every line card may cause additional failures owing to maxing out of the CPUs.

- CSCsk69194

Symptoms: The **shape average percent** calculation is wrong.

Conditions: This symptom is observed on a Cisco 7500 router that is configured for dLFIoLL. The policy is attached to ATM and multilink interfaces.

Workaround: Use only absolute values in the shape policy.

- CSCsk89546

Symptoms: OSPF routes are not populated in the Routing Information Base (RIB) with the next hop as traffic engineering (TE) tunnels.

Conditions: Occurs when multiple TE tunnels are configured and the tunnels come up or are shut/no shut simultaneously.

Workaround: Shut/no shut tunnels one at a time.

- CSCsl05174

Symptoms:

- Issue 1: A non-deleted PPP configuration inside the interface reappears when the interface is created again.
- Issue 2: Some multilink configuration is not being synced to the standby (hold-queue).

Conditions: This symptom is observed when running RPR+.

Workaround: Reapply the original configuration.

Further Problem Description: Deletion of a multilink interface and subsequent creation using the same name may cause portions of the original configuration to return even if not explicitly configured. The **hold-queue** command is not being synchronized to the standby RP.

- CSCsl51616

Symptoms: The v6-vrf-lite configuration does not synch properly with the standby; hence 100 percent of the traffic is lost after an SSO switchover.

Conditions: The conditions under which this symptom is observed are unknown.

Workaround: There is no workaround.

- CSCsl61164

Symptoms: Router may crash @ipflow_fill_data_in_flowset when changing flow version.

Conditions: Occurs when NetFlow is running with data export occurring while manually changing the flow-export version configuration from version 9 to version 5 and back to version 9 again.

Workaround: Do not change the NetFlow flow version while the router is exporting data and routing traffic.

- CSCsl68227

Symptoms: An E3 linecard may drop packets larger than a certain size because of a buffer carving problem when the mtu command is used for multilink interfaces.

Conditions: This symptom is observed with images based on Cisco IOS Release 12.0(32)S10.

Workaround: Changing the MTU or reloading the linecard may clear the problem.

- CSCsl83415

Symptoms: After executing the following CLI commands (steps mentioned alphabetically) via a script (not reproducible manually), the router sometimes crashes:

Test10:

- a. clear ip bgp 10.0.101.46 ipv4 multicast out
- b. clear ip bgp 10.0.101.47 ipv4 multicast out

Test 1:

- c. show ip bgp ipv4 multicast nei 10.0.101.2
- d. show ip bgp ipv4 multicast [<prefix>]
- e. config terminal

The crash does not happen for each of the following cases:

1. If the same CLI is cut and paste manually, there is no crash.
2. If the **clear cli** command is not executed, there is no crash.
3. If the **config terminal** command is not entered, there is no crash.

Conditions: The symptom occurs after executing the above CLI.

Workaround: There is no workaround.

- CSCsm80425

Symptoms: A Cisco 7200 device crashes when a policy map is applied.

Conditions: This symptom is observed when the service policy map is applied on the channelized E3 interface of a Cisco 7200 VXR router and traffic is pumped.

Workaround: Remove the service policy map.

- CSCsm96785

Symptoms: You may observe a problem which the OSPF neighbor is down after switch-over in spite of using OSPF Non-Stop Forwarding (NSF).

Conditions: This occurs with the following conditions:

- “nsf cisco” is only affected. If “nsf ietf”, this problem does not occur.
- You may observe this problem if the OSPF interface is “point-to-multipoint non-broadcast” or “point-to-multipoint”. If the interface is “broadcast”, this problem does not occur.
- When this problem occurs after switch-over, DBD packet may not be exchanged between two neighbors. And the neighbor is down in spite of NSF.

Workaround: Change the OSPF config to “nsf ietf” and change the OSPF interface to “broadcast”.

- CSCsm96842

Symptoms: The command **hold-queue length in** cannot be configured for port-channel interface.

Conditions: The symptom is observed with a Cisco 7600 series router after upgrading to Cisco IOS Release 12.2(33)SRC.

Workaround: There is no workaround.

Further Problem Description: Queueing is not supported for port-channel with a Cisco 7600 series router. The **hold-queue** is a legacy queueing command and is not supported.

- CSCso15740

Symptoms: The “set metric” clause in the continue route-map sequence is not setting metric correctly in some particular conditions. This is also applicable in case where the nexthop setting is done via route-map with a continue clause.

Conditions: The symptom is observed on a Cisco 12000 series router that is running Cisco IOS Release 12.0(32)SY4. This is platform independent. This symptom occurs if the route-map has a continue clause and the match condition does not allow the continue clause to be executed. The following route-map sequence which has to be executed will not execute properly if the metric or nexthop of the prefix are to be modified via the route-map.

Workaround: Avoid using “continue” in a route-map and modifying metric or nexthop via the following route-map sequence.

- CSCso32397

Symptoms: An unexpected reboot occurs because of a software-forced crash.

Conditions: This symptom is observed when changes are made in the policy map.

Workaround: There is no workaround.

- CSCso41824

Symptoms: A router crashes with an unexpected exception to CPUvector 300.

Conditions: This symptom is observed when you configure MPLS trunks on an 4xT3E3 SPA with FR IETF encapsulation.

Workaround: There is no workaround.

- CSCso46427

Symptoms: A device may crash when the **show clns interface** command is issued on the wrong interface.

Conditions: The symptom is observed when there are a number (around 100 or more) CLNS interfaces on the device.

Workaround: There is no workaround.

- CSCso51637

Symptoms: Router crashes.

Conditions: Router may crash in some cases after removing interface Auto-template and unconfiguring auto-mesh with large number of active mesh auto-tunnels. Currently, this crash has only been observed occasionally with internal scale test scripts and has not occurred with manual configuration.

Workaround: Wait until all auto-tunnels are down after unconfiguring auto-tunnel mesh globally, and before removing interface Auto-template

- CSCso54167

Symptoms: BGP peers are stuck with table versions of 0. BGP peers do not announce any routes to neighbors.

Conditions: Whenever the interfaces flap with online insertion and removal (OIR) multiple times, all of the BGP peers using such interfaces for peering connections encounter this issue.

Workaround: Delete and reconfigure the neighbor.

- CSCso64050

Symptoms: Policy-map outputs are not seen in standby router. The policy is attached to the VC in the standby, but no output is seen.

Conditions: The symptom is observed when an ATM PVC is created and a service policy is attached to the PVC.

Workaround: There is no workaround.

- CSCso65266

Symptoms: A customer upgraded to Cisco IOS Release 12.0(32)Sy4, and now the customer is seeing a memory leak in the BGP process. The memory leak is happening with the BGP router process at the rcache chunk memory when the route map has a “continue” clause in the configuration.

Conditions: The leak is seen when a “continue” statement is configured in an outbound route map.

Workaround: There is no workaround.

- CSCso65289

Symptoms: High CPU utilization is seen on a Cisco 12000 series Internet router caused by the “IPC Seat Manager” process.

Conditions: This symptom may be observed when the router is enabled with multicast distributed routing and has high scaled multicast configurations.

Workaround: There is no workaround.

- CSCso72996

Symptoms: A SIP601 sometimes crashes or gets an alignment error.

```
SLOT 4:Mar 17 17:59:03.877 UTC: %ALIGN-3-SPURIOUS: Spurious memory access made at
0x408C1E14 reading 0xF SLOT 4:Mar 17 17:59:03.877 UTC: %ALIGN-3- TRACE: -Traceback=
408C1E14 408C03D4 00000000 00000000 00000000 00000000 00000000 00000000
```

Conditions: The conditions under which this symptom occurs are unknown.

Workaround: There is no workaround.

- CSCso74028

Symptoms: The local PE is sending graft messages even after receiving data from the remote PE on an MVPN network.

Conditions: This symptom is observed when the graft-ack messages are lost in transit (could be due to misconfiguration/ACL, etc.).

Workaround: Fix the misconfiguration so that graft-ack messages are forwarded as expected.

- CSCso82178

Symptoms: Configuring a PBR at the E5 GE subinterface may cause buffer depletion. The buffer cannot be released except by reloading the linecard.

Conditions: This symptom is observed when a PBR is configured at the subinterface.

Workaround: There is no workaround.

- CSCso87348

Symptoms: A Catalyst 6500 or a Cisco 7600 may reload unexpectedly.

Conditions: Occurs when NetFlow is configured on one of the following:

- Cisco 7600 that is running Cisco IOS Release 12.2(33)SRC.
- Catalyst 6500 that is running Cisco IOS Release 12.2SXH.

Workaround: Disable NetFlow. This is done with the following commands:

```
no ip flow ingress
no ip flow egress
no ip route-cache flow
```

Enter the appropriate command for each subinterface for which NetFlow is currently configured.

- CSCso88575

Symptoms: MFR bundles associated with E5 channelized based SPAs will stop forwarding traffic, an mismatch of the connection identifier (CI) of the channelized SPA is seen on CI value in the shim header of the I2 rewrite.

Conditions: This problem will occur for I2vpns only on E5 channelized based SPAs.

Workaround: Enter into interface configuration mode.

Alternate Workaround: Remove and re-add the xconnect.

- CSCso89427

Symptoms: When a router reloads, the line protocol on serial interfaces will go down.

Conditions: This symptom is observed when bringing up the SPA-1XCHSTM1/OC3 or SPA-2XCT3/DS0 with a scaled configuration that has serial interfaces on all the T1s.

Workaround: There is no workaround.

- CSCso89794

Symptoms: Spurious accesses are seen when SNMP queries are performed on the router.

Conditions: This symptom occurs if SNMP queries like “snmpwalk -v2c 7.42.19.43 public .1.3.6.1.4.1.9.3.6.13.1” are performed on the router. Spurious accesses are seen.

Workaround: There is no workaround.

- CSCso92635

Symptoms: The line card on a Cisco 10720 resets when an IP phone is connected. The “%TOASTER-2-FAULT: T1 Exception summary:” message appears.

Conditions: The line card to which the Cisco Call Manager is connected to a Cisco 10720 crashes when an IP phone is connected to the network.

Workaround: The recommended approach is to upgrade the Cisco IOS software.

- CSCso93957

Symptoms: New T1s cannot be provisioned on a CT3 SPA.

Conditions: When a customer tries to create a new T1 on one of the controllers of a CT3-SPA that is inserted into a SIP-401, the following errors are displayed:

```
Router(config-controller)# t1 15 channel-group 7 timeslots 1-24
%Failed to configure channel group
Router(config-controller)#
Apr 24 22:51:05.283 UTC: %GRPSPA-3-VC_PROV_ERROR: Provision T1 15 channel group 7 of
T3 4/0/1 unsuccessful (error code 44) -Traceback= 20A640 20A748 954AA4 94DB80 94DC90
9582D0 4FF4E0 5006FC 240B7C 2563B0 13D7410 13C6F3C 2F517C SLOT 4:Apr 24 22:51:05.271
UTC: %SPA_CHOC_DSX-3-SPA_SW_ERR: SPA on Subslot 0: HDLC controller device driver
failure: Failed to start operation Software error was encountered.
-Traceback= 40031128 408B4020 408BCE40 408BD374 408BF114 408C004C 408C0ED8 408D24E0
408D25F8
```

Workaround: There is no workaround.

- CSCso93959

Symptoms: Newer SDRAM devices on the 2- and 4-port OC48 POS/RPR SPA require an additional initialization sequence as recommended by the vendor. Without this new initialization sequence, packets that go through the transit buffer in RPR/SRP mode or in subscription mode may get corrupted, or packet loss may occur.

Conditions: Card initialization after inserting the SPA or removing an unpowered shutdown.

Workaround: Perform an OIR on the SPA.

Customers are advised to upgrade to the newer image with this new initialization sequence. Newer software will be backward compatible with older SPA boards.

- CSCsq02826

Symptoms: The MDFS state of the line card stays in a “disabled” state, which may lead to multicast traffic being punted to the RP.

Conditions: This symptom may be observed with the following sequence of operation:

1. The router is booted without configuring the **ip multicast-routing distributed** command.
2. The **ip multicast-routing distributed** command is configured.

The issue will not be seen if the **ip multicast-routing distributed** command is present in the startup configuration when the router is reloaded.

Workaround: Enter the **clear ip mds linecard slot- number** command.

- CSCsq02883

Symptoms: A device crashes with ACL configurations.

Conditions: The RP will crash when the device is running low on memory or in a highly fragmented situation if an ACL/ACE is added/deleted.

Workaround: There is no workaround.

- CSCsq08131

Symptoms: Ping packets of 8180 or larger cause sourcing POS linecard/SIP to reload and remain in a boot state waiting for IPC connection.

Conditions: This symptom is observed with ping packets that are sourced from PRP2 with part number 800-27058-03.

Workaround: Reload the router.

Further Problem Description: This symptom is observed only on PRP2 with part number 800-27058-03.

- CSCsq09917

Symptoms: A crash occurs when BGP graceful restart is configured.

Conditions: In the following configuration:

```
ip vrf vfifteen
rd 15:15
import ipv4 unicast map rfifteen
route-target export 150:15
route-target import 150:15
```

Delete the RD, and then the unicast map, and then the VRF.

Workaround: There is no feasible workaround. Try to avoid doing such an operation as explained above.

- CSCsq15994

Symptoms: Low CPS may be observed.

Conditions: The symptoms are seen with PPPoA and PPPoE sessions.

Workaround: There is no workaround.

- CSCsq18916

Symptoms: A copy tftp operation failed with a Socket error when the FPD of an SPA was updated or when the SPA was reloaded, OIRed.

Conditions: This symptom is related to the number of (nnets) non-virtual interfaces on the box. Depending on that, a number of SPA reloads must be done.

Workaround:

1. Reload the SPA or the router.

2. Configure one loopback interface.

- CSCsq27365

Symptoms: A router can crash at l2tp_process_control_packet_cleanup.

Conditions: Conditions are unknown at this time.

Workaround: There is no workaround.

- CSCsq28627

Symptoms: CPU hogs are seen in a 1-port E3 channelized OC48.

Conditions: This symptom is observed when any of the following is done:

- **controller shut/no shut**
- **mic reload <slot>**
- **hw-mod slot <xx> shut/no shut**
- **hw-module slot <xx> reload**

Workaround: There is no workaround.

- CSCsq42001

Symptoms: The following error messages appear:

```
SLOT 5:*May 9 21:43:48.547: %LC_SPA_DMLP-1-SPAHWBUNDLEERROR: Could not perform
required operation in SPA H/w for bundle Multilink2 in bflc_cx3_dmlp_frag_on_off SLOT
5:*May 9 21:44:10.727: %SPA_CHOC_DSX-3-ERROR: Multilink2 (cmd 203) Serial5/0/1/8:0:
response parsing failed. chnl 36, bid 1 -Traceback= 40031008 408924C0 4072B1BC
40899F64 4033DB90 4033E190 4033E5C0 4033E930 4033F448 4033F600 4015B53C 4015C020 SLOT
5:*May 9 21:44:10.735: %LC_SPA_DMLP-3-CFG_FAIL: bundle Multilink2 (id 1): bay 0 err
7 (del rx link)
```

Conditions: When we remove/add/remove all members from all the configured MLP bundles once or several times, these tracebacks are seen.

Workaround: There is no workaround.

Further Problem Description: spabrg EFC mapping goes to a mismatch state, and the following is seen:

```
SLOT 5:*May 9 21:59:26.771: %SPA_CHOC_DSX-3-HDLC_CTRL_ERR: SPA 5/0: 20 TX Chnl Queue
Overflow events on HDLC Controller were encountered.
```

- CSCsq42803

Symptoms: The **hw-module slot x qos account layer2 encapsulation** command does not take effect for an AToM connection.

Conditions: This symptom is observed when xconnect is configured under a VLAN.

Workaround: There is no workaround.

- CSCsq44052

Symptoms: When configuring “is-type level-1” under “router isis”, the following error message may be received:

```
% Ambiguous command: "is-type level-1"
```

Conditions: The symptom is observed when configuring “is-type level-1” under “router isis”.

Workaround: There is no workaround.

- CSCsq44598

Symptoms: A PA-POS-2OC3 experiences an output stuck condition.

Conditions: This issue is sporadic in nature and is sometimes seen with QoS configurations although QoS is not the cause of the issue. The issue is due to an extra interrupt, which is confusing the driver if it expires before the FIFO reaches the low point. For example, if the FIFO goes full but is filled with large packets, then it is possible that the no traffic timer will expire before the tx packets have emptied. It is a communication issue between the hardware and the driver code.

Workaround: There is no workaround.

- CSCsq45502

Symptom: Serials that are part of MLPPP/MFR remain in a down state.

Conditions: This symptom is observed when T1 controllers remain down.

Workaround: There is no workaround.

- CSCsq49823

Symptoms: MDFS may get disabled in a scaled mVPN environment that has many global mroutes. Once disabled, it may keep on changing between the “active” and “disabled” states. Linecard CPU utilization may also go high.

Conditions: This symptom is observed with a Cisco IOS Release 12.0(32)S10 image.

Workaround: There is no workaround.

- CSCsq52048

Symptoms: Router crashed while running the **show vpdn tunnel all** command.

Conditions: When there are thousands of L2TP tunnels coming up, going down, running the **show vpdn tunnel all** command may result in a crash.

Workaround: There is no workaround.

- CSCsq55258

Symptoms: After a router reloads, sometimes the configuration for the gigE and POS OC12 SPA is lost from the running configuration.

Conditions: This symptom is observed when the router is reloaded.

Workaround: There is no workaround.

- CSCsq58341

Symptoms: If both L2 and L3 services co-exist on the same interface, you can no longer configure urpf on the L3 subinterface after the fix for CSCsl09772. After the router reloads, the **urpf** command will be erased from the L3 subinterface. You have to use the workaround to reapply the **urpf** command.

Conditions: This symptom is observed when both L2 and L3 services are configured on the same interface.

Workaround: Do the following:

1. Remove the L2 connection.
2. Add urpf on the L3 subinterface.
3. Re-add the L2 connection.

- CSCsq62703

Symptoms: Intermediate System-to-Intermediate System (IS-IS) tries to access invalid memory address and may cause router to stop working.

Conditions: Occurs when a switch over happens and standby router becomes active.

Workaround: There is no workaround.

- CSCsq62803

Symptoms: CPU Hog and related tracebacks are seen from the E3 Gig linecard.

Conditions: Attach a scaled policy/LC reload/router reload.

Workaround: There is no workaround.

- CSCsq67266

Symptoms: The **pos delay triggers line** command is configurable at the interface level of E3 channelized POS interfaces.

Conditions: This symptom is observed on a Cisco 12416 Internet series router that is booted with the Cisco IOS Release 12.0(32)S nightly build of 05/19/08. The router contains an E3 CHOC48 linecard.

Workaround: There is no workaround.

- CSCsq68156

Symptoms: FRF12 packets are dropped by a PE router.

Conditions: This symptom is observed on a Cisco 12000 series Internet router that has a SPA-1XCHSTM1/OC3, SPA-2XCT3/DS0, or SPA-8XCHT1/E1.

Workaround: There is no workaround.

- CSCsq71212

Symptoms: EFC clock interrupts are causing a line card to crash.

Conditions: The conditions under which this symptom occurs are unknown.

Workaround: There is no workaround.

- CSCsq77603

Symptoms: The RP crashes.

Conditions: With a map-class that has an egress policy with iphc action, dlci removal is done.

Workaround: Ensure that the map-class is removed and then dlci removal is done.

- CSCsq80773

Symptoms: Slow-path multicast fragmentation is not happening correctly. One of the output interfaces is not receiving the packets in case of MVPN traffic.

Conditions: This symptom is observed with MVPN traffic with fragmentation on one of the interfaces on E5.

Workaround: There is no workaround.

- CSCsq83540

Symptoms: A Cisco 12000 works as a PE, and an Eng5 SIP line card is used to face the CE. In the VRF, the default route 0.0.0.0 is learned from the remote PE. When the problem occurs, all traffic from the CE that is forwarded via the VRF default route is dropped.

Conditions: This symptom is observed on a Cisco 12000 Eng5 SIP line card that is running Cisco IOS Release 12.0(32)SY04, 12.0(32)SY05, or 12.0(32)SY06. When VRFs are created and deleted, new VRFs that are created will have a problem if they are allocated with a table ID allocated for older deleted VRFs.

Workaround:

1. Reload the ingress Eng5 line card that is facing the CE.

or

2. If the customer does not want to reload the line card, a second workaround can be attempted, but it is not a reliable workaround and may not always be successful. Create a new VRF without removing any VRFs, which gets a new table ID, and apply the VRF configuration completely wherever the old VRF configuration is applied.

Further Problem Description: This problem cannot be cleared by using the **clear cef linecard x** or **clear ip route vrf xxx 0.0.0.0** commands.

- CSCsq91217

Symptoms: A heartbeat failure causes SPAs to go out of service.

Conditions: This symptom can be observed under the following conditions:

1. Provision/unprovision the MFR with QoS attached to its subinterfaces with traffic.
2. Add/remove of QoS policy tried on MFR subinterfaces with queues having packets.
3. Link is swapped from MLPPP to MLFR.

Workaround: Reload the line card.

- CSCsq93004

Symptoms: Removal of a subinterface may cause memory corruption or a crash. The symptoms are unpredictable.

Conditions: The symptoms are rare and will only be observed if a sub- interface is configured for **mpls traffic-eng auto-tunnel primary use**, and the sub-interface is later removed from the configuration.

Workaround: Do not remove sub-interfaces.

- CSCsq96425

Symptoms: MVPN inner packet with IP option causes depletion of FrFab buffers of Cisco 12000-SIP-401.

Conditions: This symptom occurs on Cisco 12000 routers that are running the c12kprp-k4p-mz.120-32.SY2g image and with Cisco 12000-SIP-401. This is triggered by multicast traffic.

Workaround: Only a reload of the card solves the problem.

- CSCsr08476

Symptoms: Trying to remove the MFR bundle crashes the router.

Conditions: After OIR, remove the VIP (those VIP interfaces are members of MFR bundle). Try to remove the MFR bundle.

Workaround: There is no workaround.

Further Problem Description: The MFR bundle has one Channelized PA interface as a member. OIR remove that PA seated VIP and next try to remove the bundle using the **no int MFR** command. The router crashes.

- CSCsr09376

Symptoms: After a router reloads, the SPAs on a SIP601 may take twice as long to come up in OK mode. When this occurs, you also experience the problem that is documented in CSCsq55258.

Conditions: This symptom is observed after a router reloads.

Workaround: There is no workaround.

- CSCsr11332

Symptoms: In rare situations, the **show controller SONET port** command might crash the RP.

Conditions: This symptom has been observed on a 4CHOC12/DS3-I-SCB= line card, but it can be seen on other similar channelized line cards. It may be reproducible by executing the **show controller SONET port** command on a nonexistent port like sonet 3/4 (that is, only sonet 0/0, 0/1, 0/2, and 0/3 are valid on a 4CHOC line card). When the problem can be seen, the CLI help indicates an incorrect unit number:

```
Router# show controller sonet 12/?  
<0-48> Controller unit number
```

If the controller unit number is shown fine (for example, <0-3>), then the crash will not occur.

Workaround: There is no workaround.

- CSCsr13314

Symptoms: The **pos delay triggers line** command is configurable on APS-enabled interfaces of E3 clear channel POS line cards. After the commit of CSCsq45452, the **pos delay triggers path** command is not configurable on APS-enabled interfaces of E3 channelized POS line cards.

Conditions: This symptom is observed on a Cisco 12000 series Internet router that is booted with Cisco IOS Release 12.0(32)S. The router contains ISE OC48 POS and ISE CHOC48 POS line cards.

Workaround: There is no workaround.

- CSCsr13521

Symptoms: Memory chunk allocated for LDP-IGP Sync may leak.

Conditions: The symptom is observed on a router with a dual link to its neighbor. LDP and LDP Graceful Restart are enabled on both routers. When LDP is disabled and re-enabled globally on the neighbor router, a small memory leak occurs on this router.

To verify the memory leak, on Router 1, enable memory leak debug with the **set memory debug incremental starting-time** command. On Router 2, disable LDP globally with the **no mpls ip**. Wait for LDP session go down, then re-enable LDP. On Router 1, the memory chunk leak for LDP should be seen with the **sh mem debug leaks chunks** command.

Workaround: There is no workaround.

- CSCsr18851

Symptoms: When the router reloads, it loses the previously configured wavelength configuration and puts the controller at its default wavelength (channel 3), which is an undesirable behavior.

Conditions: This symptom is observed with Cisco IOS Release 12.0(33)S01 and an SPA-1X10GE-L-ITUC when a specific wavelength in the controller is configured (for example, wavelength itu-channel 41), the **write memory** command is issued, and then the router is reloaded.

Workaround: There is no workaround.

- CSCsr20377

Due to an eng3 HW limitation, there is more overhead added to like to like ethernet PW or ethernet interworking PW if “hw-module slot <> qos account layer2 encapsulation length <>” is configured. *without* the fix of CSCsq42803, the overhead impact is less. Request a return to the behavior of 12.0(32)SY back to pre-CSCsq42803.

- CSCsr22043

Symptoms: A controller goes into an admin down state.

Conditions: This symptom is observed when an STS path under the SONET controller is shut down.

Workaround: Perform a no shutdown on the controller.

- CSCsr27734

Symptoms: The standby router crashes.

Conditions: This symptom is observed when a service-policy map is removed from a VC.

Workaround: There is no workaround.

- CSCsr27794

Symptoms: BGP does not generate updates for certain peers.

Conditions: BGP peers show a neighbor version of 0 and their update groups as converged. Out queues for BGP peers are not getting flushed if they have connection resets.

Workaround: There is no workaround other than entering the **clear ip bgp *** command.

- CSCsr42364

Symptoms: All line cards may crash after a switchover in Route Processor Redundancy Plus mode.

Conditions: This issue is observed on Cisco 12000 series Internet routers with PRP2 processors. This issue usually requires multiple line-card reloads prior to the switchover. It is seen under conditions of high line-card utilization.

Workaround: There is no workaround.

- CSCsr47477

Symptoms: After a router reloads, sometimes there may be mbus message gets timed out on the SIP601 located in the lower cage of a Cisco 12816.

Conditions: This symptom is observed after a router reloads.

Workaround: There is no workaround.

- CSCsr47795

Symptoms: After flapping the interfaces, the FIB converges and points to the correct outgoing interface, while the FIB in hardware points to another interface.

The trigger is when the interface is flapping because the default route is updated. The BGP session is always stable and never goes down.

Topology:

End customer -----(eng3)slot4 c12k_Lab_router-42 slot5 and slot6(Eng5) ----- router_B -----
Internet

The Lab-router-42 router receives a default route from the router_B neighbor.

Snapshots from the Eng3 line card on slot4:

```
Lab-router-42# exec slot 4 show ip hardware-cef 10.1.1.1 detail
```

```
===== Line Card (Slot 4) =====
Root: 0x240CE000 Location: 0x240CE404 Data: 0x81819380 Offset: 0x93D96404 Leaf
pointer: 0x300C9C00
Leaf FCR 2 Addr 0x300C9C00 : 0xE0000100 0x0285C008 found 2 deep SRAM Loadbalance addr
0x28170020 default alpha ip loadbalance: 0x28170020 (0 paths, hw maxpath 0) Hash 1:
alpha adjacency: 0x2001FA60 (cef adj NULL or alpha_default_lb) [0] oi 0x200006 oq 4080
in A ab 50 hl 20 gp 19 tl 4 loq 9800 6/0/0 mtu 1520 Output interface is
GigabitEthernet6/0/0 <== Here ^^^^^ Here
1 tag: 23 current counters 95059, 5157246 last reported 93252, 5059668
```

```
Output Queue / Local Output Queue Bundle: [0-7] output queue 0x4080 local output queue
0x9800 PLU leaf data: 0xE0000100 0x0285C008 0xA1020304 0xA5080000 Mask bits: 1 Origin
AS: 0 Source lookup drop: yes QOS group: 0 Traffic index: 0 Precedence not set Default
Route: yes PBR enabled: no
```

While the FIB was updated to the proper outgoing interface.

```
LAB_router_42# exec slot 4 show ip cef 10.1.1.1
```

```
===== Line Card (Slot 4) =====
0.0.0.0/0, version 38, epoch 0, cached adjacency 10.125.72.74 0 packets, 0 bytes Flow:
AS 0, mask 0 tag information from 10.38.192.6/32, shared, all rewrites owned local
tag: 34 via 192.168.225.0, 0 dependencies, recursive next hop 10.125.72.74,
GigabitEthernet5/0/0 via 192.168.225.0/24 (Default) <=== HERE valid cached adjacency
tag rewrite with Gi5/0/0, 10.125.72.74, tags imposed {} <=== HERE LAB_router_42#
```

Conditions: This symptom is observed when there is a default route configured while running Cisco IOS Release 120(32)SY4 or 120(32)SY6 on Eng3.

Workaround: Enter clear ip route 0.0.0.0 or <default-network>.

- CSCsr62931

Symptoms: Cisco 7500 and 10700 builds are breaking.

Conditions: The fix for CSCsq11643 is causing build breakage.

Workaround: There is no workaround.

- CSCsr64998

Symptoms: Low BGP keepalive timer sessions flap too often during periods of high CPU utilization.

Conditions: This symptom is observed when low BGP keepalive timers are set (for example, 20/60, 10/30, 1/3). This symptom is specific to Cisco IOS Release 12.0S and 12.4T.

Workaround: Do not configure very aggressive BGP keepalive timers. Also, try not to overload the CPU.

- CSCsr65767

Symptoms: MVPN traffic is being punted to the slowpath for packets that have a size ranging from 1476 to 1500 (minimum IP MTU of the outgoing interfaces is 1500).

Packets that have a size ranging from 1476 to 1500 are being punted to the slowpath, which is not required. During the fragmentation check, we should check the packet size with:

1) Minimum IP MTU of customer-facing interfaces.

2) Minimum IP MTU of core-facing interfaces - gre header (24).

If the size is greater than the above value, then only the packet should be punted to the slowpath for fragmentation.

Conditions: This issue applies to the MVPN on the Cisco 12000 series Internet router with an E5 line card as the egress line card. The issue is not seen with an E3 line card.

Workaround: There is no workaround.

- CSCsr70530

Symptoms: A line card crashes.

Conditions: This symptom is observed after members of the MLPPP are swapped from one bay to another bay and vice-versa on the same line card.

Workaround: There is no workaround.

- CSCsr70985

Symptoms: A Cisco router crashes following multiple accesses to NVRAM.

Conditions: This symptom has been observed on a Cisco 12000 series Internet router that is running Cisco IOS Release 12.0(32)SY5 when the “dir tar:” command is executed parallel with the “write memory” command. It may not be platform specific.

Workaround: Avoid using the “dir tar:” command.

- CSCsr71139

Symptoms: The following messages are displayed in the syslog:

```
%QM-4-SW_SWITCH: Interface GigabitEthernet7/0/1.558 routed traffic will be software  
switched in egress direction(s)
```

Another symptom is that the “show policy-map interface” command for the affected interface displays “Class of service queue: 0” for all queues.

Conditions: These symptoms are observed on Engine 5 line cards when attaching to an interface a policy map that requires more WRED resources than what is available in the line card.

Workaround: Verify whether the line card has enough WRED resources available before attaching a new policy map to one of its interfaces.

Further Problem Description: On Engine 5 line cards, when attaching to an interface a policy map that requires more WRED resources than what is available in the line card, no verification for available WRED resources is performed and the command is accepted. This is because Engine 5 line cards, as opposed to Engine 3 line cards, have Line Card Based QoS Manager. Because the policy cannot be programmed in hardware (there are not enough RED resources), the traffic is punted to the line card CPU (that is, it is software-switched). This fix makes the error message more prominent.

- CSCsr79573

Symptoms: The member link of a multilink bundle goes into an up/down state.

Conditions: This symptom is observed when multilink is swapped from one multilink bundle to another multilink bundle through a script.

Workaround: Enter the “hw-module subslot <slot#/subslot#> reload” command.

- CSCsr80321

Symptoms: Commands cannot be sent to the SPA.

Conditions: This symptom is observed when the members of MLPPP and MLFR are swapped.

Workaround: Reload the line card.

- CSCsr83626

Symptoms: The line card in slot 0 does not boot up completely. It does not go past the UP IOS state.

Conditions: This symptom is observed after upgrading the router to Cisco IOS Release 12.0(32)SY5 and having the ATM line card in slot 6 send an LAIS alarm.

Workaround: Move the ATM card to another slot, or shut down the ATM line card in slot 6.

- CSCsr85656

Symptoms: On removal of an xconnect from the L2 transport PVC (ATM portmode), the policy map is not removed and entries still exist.

Conditions: This symptom is observed when an xconnect is removed from the L2 transport PVC (ATM portmode).

Workaround: Remove the policy map first and then remove the xconnect configuration.

- CSCsr99670

Symptoms: Channelized SPAs on Engine-5 line cards might go to out-of-service.

Conditions: There should be all kinds of interfaces (with encapsulations hdlc/ppp/fr/gige l2fwding enabled on some interfaces) in the same Engine-5 line card.

Workaround: Reload the Engine-5 line card.

- CSCsr99774

Symptoms: An engine 5 line card is queueing on egress the GRE precedence rather than the original IP packet precedence.

Conditions: This symptom is observed under the following conditions:

1. Send MVPN traffic.
2. Configure an egress QoS policy on the decap side.
3. Configure a QoS policy in the core to set the GRE IP precedence.

Workaround: There is no workaround.

- CSCsu09595

Symptoms: A SIP-601 crashes while changing the CRC/encap/MTU on MLPPP and MFR.

Conditions: This symptom is observed under the following conditions:

1. Change the CRC of the members of the bundle (from crc 16 to 32 and then back again to crc 16).
2. Remove the members from the bundle.
3. Add serials back to MFR and MLPPP.
4. Change the MTU.
5. Flap the links (serials and bundle).

Workaround: There is no workaround.

- CSCsu12040

Symptoms: BGP neighbors that are configured with as-override and send-label (CsC) together may not work after an interface flap or service reset.

Conditions:

neighbor xxx as-override neighbor xxx send-label

Workaround: Enter the “clear ip bgp * soft in” command.

Further Problem Description: Peers (neighbors) with a CsC (IPv4+label) BGP configuration with the as-override option should be separated into different dynamic update groups during the BGP update generation process. After the CSCef70161 fix in Cisco IOS Release 12.0(32)SY4, this is no longer the case; this CSCsu12040 fix enhances the CSCef70161 fix to handle the CsC (IPv4+label) case separately.

- CSCsu12146

Symptoms: On a Cisco 12404 that is running Cisco IOS Release 12.0(32)SY5, a SIP-401 reloads when lawful intercept (LI) is used on it.

Conditions: This symptom is observed when LI is activated.

Workaround: Deactivate LI.

- CSCsu21668
Symptoms: “carve-level 0” is being used in SY5 nodes (SIP-601) to avoid unnecessary buffer recarving and subsequent traffic disruption.
Conditions:
carve-level 0
Workaround: There is no workaround.
- CSCsu41968
Symptoms: On a Cisco 7500 with an HA setup, the “show controller t3” command is showing framing as M23 on the active and as C-bit on the standby. So the “loopback remote” configuration is rejected on the active and is accepted on the standby.
Conditions: This symptom is observed when the “show controller t3 1/1/0” command is issued.
Workaround: There is no workaround.
Further Problem Description: Because of the framing mismatch, the standby might crash due to sync issues.
- CSCsu45425
Symptoms: Label Forwarding Information Base (LFIB) shows incorrect information for Global BGP prefix after route flap. LFIB/FIB shows prefix as having a tag when it should be not. Routing table is correct.
Conditions: Occurred on a Cisco 12000 router running Cisco IOS Release 12.0(33)S1.
Workaround: Enter the **clear ip route** command.
- CSCsu86371
Symptoms: The connect command that is used to configure FRoMPLS is rejected.
Conditions: This symptom is observed with E0/E2 cards and E3/E5 MFRs.
Workaround: There is no workaround.
- CSCsv04345
Symptoms: A GRP crashes with DWDM.
Conditions: This symptom is observed when the “show controllers dwdm” command is issued.
Workaround: There is no workaround.
- CSCsv21489
Symptoms: Traffic is dropped on an FR subinterface with IPHC configurations when the SPA reloads.
Conditions: This symptom is observed when IPHC is configured.
Workaround: Shut/no shut the affected main interface (for the subinterfaces).
- CSCsv30035
Symptoms: ICMP packets get corrupted when PXF is enabled.
Conditions: This symptom is observed when PXF is enabled.
Workaround: Disable PXF.

Resolved Caveats—Cisco IOS Release 12.0(33)S1

All the caveats listed in this section are resolved in Cisco IOS Release 12.0(33)S1. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCeb69473

Symptoms: Device crashes with a segmentation violation (SegV) exception.

Conditions: Occurs when the **connect target_ip [login|513] /terminal- type value** command is entered with a large input parameter to the *terminal-type* argument such as the following:

```
router>connect 192.168.0.1 login /terminal-type aaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

Trying 192.168.0.1...Open login:

```
*** System received a SegV exception *** signal= 0xb, code= 0x1100, context= 0x82f9e688 PC =
0x61616160, Vector = 0x1100, SP = 0x833ae5a8
```

Workaround:

AAA Authorization AAA authorization enables you to limit the services available to a user. When AAA authorization is enabled, the network access server uses information retrieved from the user's profile, which is located either in the local user database or on the security server, to configure the user's session. Once this is done, the user will be granted access to a requested service only if the information in the user profile allows it.

For a complete description of authorization commands, refer to the following links:

Configuring Authorization

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hsec_c/part05/schathor.htm

ACS 4.1 Command Authorization Sets

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.1/user/SPC.html#wp480029

ACS 4.1 Configuring a Shell Command Authorization Set for a User Group

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.1/user/GrpMgt.html#wp480029

Role-Based CLI Access The Role-Based CLI Access feature allows the network administrator to define "views," which are a set of operational commands and configuration capabilities that provide selective or partial access to Cisco IOS EXEC and configuration (Config) mode commands. Views restrict user access to Cisco IOS command-line interface (CLI) and configuration information; that is, a view can define what commands are accepted and what configuration information is visible. Thus, network administrators can exercise better control over access to Cisco networking devices. The following link provides more information about the Role-Based CLI Access feature:

Role-Based CLI Access

http://www.cisco.com/en/US/netsol/ns696/networking_solutions_white_paper09186a00801ee18d.shtml

Device Access Control Due to the nature of this vulnerability, networking best practices such as access control lists (ACLs) and Control Plane Policing (CoPP) that restrict vulnerable device access to certain IP addresses or Subnetworks may not be effective. Device access best practices provide some mitigation for these issues by allowing systemic control of authenticated and unauthenticated users. Device access best practices are documented in:

Infrastructure Protection on Cisco IOS Software-Based Platforms Appendix B-Controlling Device Access

http://www.cisco.com/application/pdf/en/us/guest/products/ps1838/c1244/cdccont_0900aecd804ac831.pdf

Improving Security on Cisco Routers <http://www.cisco.com/warp/public/707/21.html>

- CSCee29138

Symptoms: The `ciscoMemoryPoolType` returns the wrong value for all memory types, except processor.

Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.2 S, 12.3, or 12.3 T.

Workaround: There is no workaround.

- CSCek63384

Symptoms: A service policy is unexpectedly removed.

Conditions: This symptom is observed when you apply a service policy to a multilink interface and then the interface is reset.

Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, reconfigure the service policy after the multilink interface has been brought up.

- CSCek78237

Symptoms: A short CPU hog seen in the ATM PA Helper process when an interface flaps and the framing configuration is modified on the interface.

Conditions: This symptom is observed on a Cisco 7200 with a PA-A3-T3 adapter that is running Cisco IOS Release 12.2(25)S or 12.2(31)SB (and possibly other Cisco IOS releases).

Workaround: There is no workaround.

Further Problem Description: The CPU hog is enough to cause OSPF adjacencies (with fast hello) to go down on other unrelated interfaces. The same problem is seen if BFD is configured.

- CSCek79178

Symptoms: The **`dot1q tunneling ethertype 0x9100`** interface configuration command disappears from the main interface after a route processor (RP) switchover.

Conditions: This symptom is observed after an RP switchover.

Workaround: There is no workaround.

- CSCsb63652

Symptoms: BGP convergence is very slow, and CPU utilization at the BGP Router process is always near 100 percent during the convergence at the aggregation router. This issue obviously shows the following tendencies:

- 1) The greater the number of component prefixes that belong to the aggregate- address entry, significantly slower convergence is seen at the aggregation router.
- 2) The greater the number of duplicate aggregation component prefixes for the aggregate-address entry, seriously slower convergence is seen at the aggregation router.

Conditions: Any release would be affected if "aggregate-address" is configured and routing updates are received every few seconds.

Workaround: Remove the "aggregate-address".

Further Problem Description: If you configure "aggregate-address" lines after BGP convergence has been achieved, the BGP process only holds about 60 or 80 percent of the CPU for about 1 minute. However, if you do peer reset after "aggregate-address" entries have been configured, the convergence time is about 32 minutes (it is about 6 minutes if "aggregate-address" entries are removed).

- CSCse50781

Symptoms: After executing the **no ipv6 multicast-routing** command on a dual-RP router, IPC communication to the standby RP may be broken, and the following messages may be seen every minute:

%IPCGRP-3-ERROR: standby set time: timeout seen

Conditions: This symptom is observed on a Cisco 12000 series router that is running the c12kprp-p-mz image of Cisco IOS Release 12.0(32)SY.

Workaround: Reload the router.

Further Problem Description: This bug is seen only while operating in SSO mode (not in RPR mode).

- CSCse56501

A device running Cisco IOS software that has Internet Protocol version 6 (IPv6) enabled may be subject to a denial of service (DoS) attack. For the device to be affected by this vulnerability the device also has to have certain Internet Protocol version 4 (IPv4) User Datagram Protocol (UDP) services enabled. To exploit this vulnerability an offending IPv6 packet must be targeted to the device. Packets that are routed throughout the router can not trigger this vulnerability. Successful exploitation will prevent the interface from receiving any additional traffic. The only exception is Resource Reservation Protocol (RSVP) service, which if exploited, will cause the device to crash. Only the interface on which the vulnerability was exploited will be affected.

Cisco is providing fixed software to address this issue. There are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20080326-IPv4IPv6.shtml>

- CSCse75697

Symptoms: When an ATM interface is configured with an IMA group and when you enter the **clock source line** command, the router may crash.

Conditions: This symptom is observed on a Cisco router that integrates the fixes for caveats CSCin90422 and CSCsb68536.

Workaround: There is no workaround.

Further Problem Description: The symptom occurs because the default clocking has been changed to "internal" via the fixes for caveats CSCin90422 and CSCsb68536. The fix for this caveat, CSCse75697, sets the default clocking back to "line."

- CSCse92050

Symptoms: A router may reload unexpectedly when a routing event causes multicast boundary to be configured on a Reverse Path Forwarding (RPF) interface.

Conditions: This symptom is observed on a Cisco platform that is configured for PIM.

Workaround: Remove multicast boundary from the configuration.

- CSCsg08751

Symptoms: Route Switch Processor (RSP) may crash when flash card is removed from RSP slot.

Conditions: This has been seen on RSP running Cisco IOS Release 12.4(10).

Workaround: There is no workaround.

- CSCsg35077

Symptoms: A device that is running Cisco IOS software may crash during processing of an Internet Key Exchange (IKE) message.

Conditions: The device must have a valid and complete configuration for IPsec. IPsec VPN features in Cisco IOS software that use IKE include Site-to-Site VPN tunnels, EzVPN (server and remote), DMVPN, IPsec over GRE, and GET VPN.

Workaround: Customers that do not require IPsec functionality on their devices can use the **no crypto isakmp enable** command in global configuration mode to disable the processing of IKE messages and eliminate device exposure.

If IPsec is configured, this bug may be mitigated by applying access control lists that limit the hosts or IP networks that are allowed to establish IPsec sessions with affected devices. This assumes that IPsec peers are known. This workaround may not be feasible for remote access VPN gateways where the source IP addresses of VPN clients are not known in advance. ISAKMP uses port UDP/500 and can also use UDP/848 (the GDOI port) when GDOI is in use.

Further Problem Description: This bug is triggered deep into the IKE negotiation, and an exchange of messages between IKE peers is necessary.

If IPsec is not configured, it is not possible to reach the point in the IKE negotiation where the bug exists.

- CSCsg42672

Symptoms: On a Cisco router running Cisco IOS Release 12.0(32)S4 and configured with BGP and peer-groups, if the Fast Peering Session Deactivation feature is configured in the peer-group, the router automatically configures on the command a route-map with the same name as the peer-group.

Conditions: Occurs with the following configuration sequence:

```
RR#conf t Enter configuration commands, one per line. End with CNTL/Z. RR(config)#router bgp 65001
RR(config-router)#neighbor rrs-client fall-over ? bfd Use BFD to detect failure route-map
Route map for peer route <cr>
```

```
RR(config-router)#neighbor rrs-client fall-over
```

```
RR#sh ru <snip> router bgp 65001
```

```
neighbor rrs-client peer-group neighbor rrs-client remote-as 20959 neighbor rrs-client
update-source Loopback0 neighbor rrs-client fall-over route-map rrs-client <<<<<<<
```

the route-map does not exist.

Workaround: Configure the neighbor individually or use peer-templates.

- CSCsh31546

Symptoms: Applying L4 operators (used with an ACL) on many interfaces at the same time generates a traceback.

Conditions: There is no set procedure for generating the traceback. You must play around with the configuration to generate it.

Workaround: Configure the ACL batch by batch; for example, 20 to 30 interfaces at a time.

- CSCsh75224

Symptoms: RP crashes in IFS code when a SSH or TELNET session is established while the switch is attempting to download a configuration.

Conditions: Occurs on a Cisco Catalyst 6509.

Workaround: There is no workaround.

- CSCsj12867

Symptoms: The following message can be seen after executing the **write memory** command, even though the version has not been changed.

Router# write memory

Warning: Attempting to overwrite an NVRAM configuration previously written by a different version of the system image. Overwrite the previous NVRAM configuration?[confirm]

The router then restarts with the following traceback:

```
-Traceback= 6067F3DC 6067FB38 605E3FE8 60686384 605E3FE8 605188BC 60518830  
605444D4 60539164 6054719C 605AB65C 605AB648
```

Conditions: This symptom is observed on a Cisco 7206 VXR (NPE-400) with C7200-IO-FE-MII/RJ45= or C7200-I/O= running the Cisco IOS Release 12.2(24a) interim build.

Workaround: There is no workaround.

- CSCsj21785

Symptoms: A Traffic Engineering (TE) tunnel does not re-optimize to explicit path after an MTU change.

Conditions: The TE tunnel is operating via explicit path. The MTU on outgoing interface is changed. OSPF is flapped, and it does not come up as there is MTU mismatch (MTU is not changed on peer router). Meanwhile the TE re- optimizes to a dynamic path-option as expected. Now the MTU is reverted back to the previous value, and the OSPF adjacency comes up. The TE tunnel does not re-optimize to explicit path. Manual re-optimization of the TE tunnel fails as well, and the TE tunnel sticks to the dynamic path.

Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the particular interface.

- CSCsj68299

Symptoms: The line card crashes when the interface MTU is changed.

Conditions: This symptom is observed when having both ingress and egress E0 cards with MPLS in the core and when an ATOM tunnel is configured on the egress line card.

Workaround: Before changing the MTU, stop the traffic across all the E0 line card interfaces. You can resume traffic after changing the MTU.

- CSCsj74173

Symptoms: Egress E0 - Two ports OC3 channelized to DS1/E1 are crashing continuously just as traffic starts.

Conditions: E0 - In an IP->Tag fragmentation case with E4/E4P/E6 POS cards as the ingress and E0 as the egress card, for certain frame sizes larger than the egress MTU, the E0 egress card crashes. This happens only with the E0 card as egress.

Workaround: Make sure that the packets sent are less than the egress MTU of the E0 linecard to avoid any fragmentation.

- CSCsj99269

Symptoms: With some VPN configurations, such as configurations with a multipath import or an import map, the CPU usage of the router may be very high for a long time, even after BGP convergence has occurred.

Conditions: This symptom is observed on a Cisco router that functions in a highly scaled environment involving several hundred VRFs and occurs after the router has been reloaded or after a switchover has occurred.

Workaround: There is no workaround.

- CSCsk10104

Symptoms: MPLS-TE tunnels do not come up after a core interface is brought down and then up again by entering the **shutdown** command followed by the **no shutdown** command.

Conditions: This symptom is observed when there are 200 MPLS-TE tunnels and 1000 VRFs configured on an NES-150 and when entering the **shutdown** command followed by the **no shutdown** command for the core interface when the traffic is on for all 1000 VRFs end to end.

Workaround: Enter the **no mpls traffic-eng tunnels** command followed by the **mpls traffic-eng tunnels** command, and all tunnels come up.

- CSCsk15805

Symptoms: If you shut down a TE tunnel interface and you have a static route through the tunnel, the routing table is not updated immediately but only when the static scan runs (every minute by default).

Conditions: This problem is fine if the static route is pointing to a physical interface and happens only with TE tunnel interfaces when it is configured with the **ip routing protocol purge** command.

Workaround: Remove the **ip routing protocol purge** command or tune the adjust timer (**ip route static adjust-time** command).

- CSCsk26165

Symptoms: A router may crash because of a bus error.

Conditions: The router must be configured for L2TP.

Workaround: There is no workaround.

- CSCsk30571

Symptoms: Field diagnostics fail (indicating a DOWNLOAD FAILURE) on the standby PRP2 when the PRP2 has 4 GB of memory installed.

After 40 minutes, the default download time limit, field diagnostics declare a download failure and reload the board. The failure message for this looks like the following:

```
----- Field Diagnostic:
****DOWNLOAD FAILURE**** while preparing slot {#}
```

```
Field Diag eeprom values: run 3 fail mode 5 (DOWNLOAD FAILURE) slot {#} last test failed was
0, error code 0 Shutting down diags in slot {#}
```

```
Board will reload -----
```

Conditions: This symptom is observed for any release of Cisco IOS software when you attempt to run field diagnostics on a standby PRP that has 4 GB of memory.

Workaround: There is no workaround.

- CSCsk34458

Symptoms: An E5 line card with a 1x10GE SPA can crash when the laser of a JDSU T-BERD 8000 testset that is connected to the 10GE interface is enabled.

Conditions: This symptom is observed on a router that contains an E5 line card with a 1x10GE SPA and redundant PRP-2 processors that are booted with the c12kprp-p-mz.12.0(32)S7 image and that are running in RPR+ mode.

Workaround: There is no workaround.

- CSCsk36276

Symptoms: Traceback seen at `tfib_post_table_change_label_request_needed`.

Conditions: Occurs during SSO switchover on a Cisco 7606 router.

Workaround: There is no workaround.

- CSCsk36552

Symptoms: Some packet flows may be dropped when the next-hop is load-shared between MPLS-TE tunnel and physical interface. The next-hop entry for the physical interface is invalid in Hardware-CEF table in ingress Line-Card during this problem. This cause the some packet flows which look up the invalid entry as the result of hash calculation to be dropped. The other flows which looks up the tunnel interface are not affected.

You can check the detail of hardware-CEF table for this problem by entering the **show ip hardware-cef prefix detail** command in Engine 3 and Engine 5.

Conditions: This problem occurs when the next-hop is load-shared between MPLS-TE and physical interface. This problem may be observed when using Engine 3 or Engin 5 as the ingress Line-Card on GSR.

Workaround: There is no workaround.

- CSCsk55692

Symptoms: A Cisco 7500 series router that is running Cisco IOS Release 12.2SB and Release 12.0S continues to witness output drops after configuring and unconfiguring an Output Policy containing Police feature on a Logical Interface. On a Cisco 7507 router that is running Cisco IOS Release 12.0(32) S9, reconfiguring fair-queue causes the VIP crash by signal = 10.

Conditions: The problem is caused when installing a policy with police on a logical interface: Subinterface, ATM PVC, Frame Relay DLCI, etc. After removal of such policy, the interface continues to police traffic. If the interface is configured with FR and the fair-queue is reconfigured, the VIP crashes.

Workaround: There is no workaround. The router has to be reloaded to correct the behavior.

- CSCsk60112

Symptoms: Uninitialized memory causes failures when label switched path (LSP) ping is performed

Conditions: This error occurs when the allocated memory is non-zero.

Workaround: There is no workaround.

- CSCsk61790

Symptoms: Syslog displays password when copying the configuration via FTP.

Conditions: This symptom occurs when copying via FTP. The Syslog message displays the password given by the user as part of syntax of FTP copy.

Workaround: There is no workaround.

- CSCsk66339

Symptoms: A Cisco 7600 router running Cisco IOS Release 12.2(18)SFX6 may encounter a condition such that when intermediate system-to-intermediate system (IS-IS) and traffic engineering (TE) are configured, IS-IS should remove the native path from its local RIB and call RIB code to remove the path from global RIB but fails by either not passing the "delete" msg to RIB properly or RIB does not react when it received the "delete" call.

Conditions: The **show mpls traffic-engineering tunnel** command output may indicate "Removal Trigger: setup timed out" status.

Workaround: Perform a **shut/no shut** on the interface or change the metric temporarily to force an update with the **tunnel mpls traffic-eng autoroute metric 1** command.

- CSCsk67111

Symptoms: Watchdog timeout seen after switchover.

Conditions: Occurs when high availability RPR mode is configured on a Cisco 7500 router.

Workaround: There is no workaround.

- CSCsk78725

Symptoms: While giving T1 controller configuration, the router crashes. This happens on the 8-port multichannel T1/E1 8PRI PA (PA-MC-8TE1+).

Conditions: Occurs on a router running Cisco IOS Release 12.4(17.7) and Cisco IOS Release 12.4(17.4)T1.

Workaround: There is no workaround.

- CSCsk81155

Symptoms: OSPFv3 loses hello packets causing neighbors to flap.

Conditions: Occurs on a Cisco GSR router running Cisco IOS Release 12.0(32)S7 and later when TE tunnels are configured.

Workaround: There is no workaround.

- CSCsk81725

Symptoms: All E6 line cards are holding incorrect output slot information in hardware CEF for default route. At the same time, other E4+ and E2 LCs have no problem with hardware CEF.

Conditions: Unknown.

Workaround: Use the **clear ip route 0.0.0.0** command.

- CSCsk82701

Symptoms: Hot Standby Routing Protocol (HSRP) Virtual IP address is unreachable. IP address assigned to the interfaces is reachable.

Conditions: Problem was seen in GSRs with different SPAs. Problem occurs only when line card is installed for the first time or if it is moved between slots. Problem only occurs if the same interface is both configured for HSRP and assigned to VPN routing/forwarding (VRF) VRF.

```
interface GigabitEthernet3/0/0.5 ip vrf forwarding ip address X.X.X.2 X.X.X.X standby 1 ip
X.X.X.1 standby 1 priority 110 standby 1 preempt
```

Workaround: Reload active and standby router as if you reload only active there is a chance standby router once become active may hit the problem. Or, remove the HSRP configuration before moving the linecard.

- CSCsk98123

Symptoms: Tx traffic may get dropped due to a "precam 1 exception."

Conditions: This symptom is observed when vrf vlite and strict urpf are configured on the interfaces. This happens in all releases when adjacency indexes between 65528 to 65531 are used in TX SRAM Adjacency programming on line cards. This happens only on port 0. Strict URPF not a required condition. It can happen without that.

Workaround: To recover from the situation, remove and re-apply the configuration on the interface when the problem is seen. To recover from the condition, shut and no shut of the interface is fine provided it does not get adjacency index allocated within 65528 and 65532. If URPF/PBR is configured or removed, then also it gets cleared.

Alternate Workaround: Do not use port 0 on the line card. Using a subinterface will mitigate the issue.

- CSCsl01921

*Some packet flows dropped in nexthop load-sharing between TAG and IP

- CSCsl03699

Symptoms: SPA-4XCT3/DS0 serial interface went down.

Conditions: Connected the shared port adapter (SPA) back to back and configured remote loopback from one router and entered **t1 1 bert channel-group 0 pattern 2^11 interval 1**. BERT ran successfully, then the serial interface went down.

Workaround: Perform a **shut/no shut** on the controller or serial interface.

- CSCsl06336

Symptoms: When the **maximum-paths n import** command is unconfigured, for example, a **no maximum-paths n import m** command is issued for a VPN/VRF on a router, sometimes the routes in that VPN may have duplicate path entries.

For example:

```
diezml#sh ip bgp vpnv4 v v1001 10.0.20.0 BGP routing table entry for 100:1001:10.0.20.0/24,
version 1342275 Paths: (2 available, best #1, table v1001) Flag: 0x420 Not advertised to any peer
65164, imported path from 100:1:10.0.20.0/24 192.168.1.7 (metric 4) from 192.168.1.254
(192.168.1.254) Origin IGP, metric 1552, localpref 80833, valid, internal, best Extended
Community: RT:100:1001 Originator: 192.168.1.7, Cluster list: 192.168.2.7 mpls labels in/out
nolabel/291 65164, imported path from 100:1:10.0.20.0/24 192.168.1.7 (metric 4) from
192.168.1.253 (192.168.1.253) Origin IGP, metric 1552, localpref 80833, valid, internal Extended
Community: RT:100:1001 Originator: 192.168.1.7, Cluster list: 192.168.2.7 mpls labels in/out
nolabel/291
```

Workaround: The least resource-intensive workaround is to configure and unconfigure a dummy import map under that VPN/VRF. Clearing the affected BGP sessions on PEs also resolves the issue.

- CSCsl07297

Symptoms: Router may crash when a sequence of commands are executed in quick succession.

Conditions: Occurs when a Border Gateway Protocol (BGP) neighbor belongs to a particular peer group and the following commands are entered in quick succession: *** no neighbor a.b.c.d peer-group pgroup-name * no neighbor a.b.c.d description xyz** If these commands executed quickly, such as when they are pasted into the interface, the router may crash.

Workaround: Use the **no neighbor a.b.c.d peer-group pgroup-name** command to remove the neighbor. This command removes the neighbor and eliminates the need for the second command.

- CSCsl09752

Symptoms: Packet drops occurring on PE router.

Conditions: Occurs after sending traffic from VPN routing/forwarding (VRF). Traffic is stopped until the mroute entries get cleared. When traffic is sent from core, packets are dropped.

Workaround: Reload the line card.

- CSCsl10053

None Symptom: After gsr is booted, up and running, when first time dwdm spa is inserted in linecard, linecard crashes. After linecard restart, next oirs are fine.

Workaround: Before gsr boots, keep dwdm spa inserted in linecard and then boot gsr.

- CSCs111335

Symptoms: The number of entries obtained from the "ciscoMvpnBgpMdtUpdateTable" table using the **getmany** command is incorrect

Conditions: Occurred on a Cisco 7200 router running Cisco IOS version 12.4(17.9)T.

Workaround: There is no workaround.

- CSCs115026

Symptoms: Configuration applied to a multilink interface is not reflected on the interface.

Conditions: Occurs when a configuration is applied immediately after adding the first link to a multilink PPP or a multilink frame-relay bundle. It affects any configuration applied to the main interface or to the sub-interface of the bundle. The problem does not occur when adding subsequent member links to the bundle.

Workaround: After adding the first link, wait 15 seconds before applying any configuration to the bundle interface or on the sub-interface. If any of the configurations are missing, re-apply them.

- CSCs116385

Symptoms: Line card reloads.

Condition: Occurs after high-availability switchover and caused by excessive number of control messages.

Workaround: There is no workaround.

- CSCs117766

Symptoms: Attempting to configure serial interfaces results in the following message and a traceback: %FIB-2-HW_IF_INDEX_ILLEGAL: Attempt to create CEF interface for Serialx/x with illegal index: -1

Conditions: When this happens the "ifindex" table appears to be incorrect on the PRP as a result of a race condition related to online insertion and removal (OIR) events. This problem should only occur if SSO or RPR+ redundancy is configured.

Workaround: If this happens on an HA-protected Active RP, check whether the Standby RP has good if- index values for all interfaces by running the **show idb EXEC** command on the Standby RP. If so, then do an RP switchover, so the RP with good interface indexes becomes the Active RP.

If the Standby RP shows this symptom, reload the Standby RP and check that after it comes up it has good if-index values, which should happen in most cases.

- CSCs118488

Symptoms: BERT continues to run on a T1 channel of SPA-1XCHSTM1/OC3.

Conditions: Occurred when a SPA-1XCHSTM1/OC3 shared port adapter (SPA) was connected back-to-back and configured with 12 T1 links with a network loopback from the other router. The following steps cause the problem:

1) Run normal bert patterns on 6 T1 channels 2) Once the bert is done run atlas bert pattern on 4 T1 channels 3) Later run atlas bert pattern on 4 T1 channels.

Workaround: Reload the SPA.

- CSCs128278

Symptoms: Routes and packets are lost.

Conditions: Occurs because NSF restart is not recognized by some of the neighbors after a router restarts.

Workaround: There is no workaround.

- CSCsl29991

Symptoms: Link is flaps after reload.

Conditions: Occurs with a Engine 5 line card and 5x1GE shared port adapter (SPA) following a reload of SPA or line card.

Workaround: There is no workaround.

- CSCsl30331

Symptom: Prefixes are allowed by the outbound route-map even though the match condition is met and the action is set to deny.

Conditions: Occurs in the following scenario: 1. The iteration with the deny action contains a match community. 2. The continue statement is used in one of the previous iterations.

Workaround: If there is single match clause based on NLRI, the condition is avoided.

Further Problem Description: Route-maps can be used without continue to avoid the problem.

- CSCsl31683

Symptoms: PC error messages are seen along with tracebacks and SPA console is not available while running atlas BERT.

Conditions: The issue is seen when running atlas BERT on CHSTM1.

Workaround: Reload the SPA

- CSCsl31789

Symptom:

RP Crashed with MLPPP Provisioning / unprovisioning -- followed by SPA reload

Conditions:

RP Crashed with MLPPP Provisioning / unprovisioning -- followed by SPA reload

Workaround:

- CSCsl32142

Symptoms: A router may reload after reporting SYS-3-OVERRUN or SYS-3-BADBLOCK error messages. SYS-2-GETBUF with 'Bad getbuffer' error may also be reported.

Condition: Occurs when PIM auto-RP is configured and IP multicast boundary is enabled with the **filter-autorp** option.

Workaround: Configure IP multicast boundary without the **filter-autorp** option.

- CSCsl32220

Symptoms: Cisco 12000 router running Cisco IOS Release 12SY may experience intermittent communications problems over Bridged VCs and ARP entries are not repopulated.

Conditions: Occurs when VC is configured for half-bridging and the router is running Cisco IOS Release 12.0SY.

Workaround: Use Cisco IOS Release 12.0S or, use VCs with routed encapsulation.

- CSCsl33471

Symptoms: Anyphy value changes after channel group BERT.

Conditions: Anyphy value changes after channel group BERT for an interface if another interface on the same SPA with a lower anyphy value is deleted.

Workaround: Reload the line card.

- CSCsl36013

Symptoms: A Cisco 12000 series router with an Engine 0 ATM OC12 line card may experience a problem in which a Layer 2 adjacency rewrite string for an ATM PVC becomes invalid. The invalid rewrite results in packets being forwarded out the interface with the wrong Layer 2 details prepended.

Conditions: This symptoms is observed on a Cisco 12000 series router with an Engine 0 ATM OC12 line card.

Workaround: Use the following command for the affected IP address:

```
clear ip arp x.x.x.x
```

Further Problem Description: This problem can be identified using the **execute-on [slot#] show controller rewrite** Cisco IOS command, compared to the rewrite string in the **show adjacency internal** command:

```
Router# execute-on 1 show controller rewrite
```

```
===== Line Card (Slot 1) =====
```

```
Local MAC rewrite table Interface Address Output_Info
```

```
----- ... ATM1/0.1 192.168.1.1 0x1C062340
4BA72000AABA031180C2000700000004 757122D600081008B0560800 <-- incorrect ...
```

```
Router# execute-on all show adjacency internal
```

```
===== Line Card (Slot 1) =====
```

```
Protocol Interface Address ... IP ATM1/0.1 192.168.1.1(9) 131229862 packets, 74135640171 bytes
02710100AABA031180C2000700000017 E0DC040200072009B0450800 <-- correct ...
```

```
Router# clear ip arp 192.168.1.1
```

```
Router# execute-on 1 show controller rewrite
```

```
===== Line Card (Slot 1) =====
```

```
Local MAC rewrite table Interface Address Output_Info
```

```
----- ... ATM1/0.1 192.168.1.1 0x1C025340
6EA82000AABA031180C2000700000017 E0DC040200072009B0450800 <-- correct ...
```

- CSCsl36723

Symptoms: A SIP401/SIP600 may crash upon a primary CSC failover. FIA Halt related error messages are also seen.

Conditions: This symptom is observed upon a primary CSC failover.

Workaround: There is no workaround.

- CSCsl41107

Symptoms: When explicit-null packets are received on URPF bundle, there is a possibility of BMA errors and crash.

Conditions: Occurs when explicit-null and URPF are configured.

Workaround: There is no workaround.

- CSCsl43394

Symptoms: Standby RSP reloads and has problems syncing configuration when DS1 controller is removed from DS3 configuration.

Conditions: This problem is seen when SSH is enabled on the router and DS1 controller is added or deleted from the configuration.

Workaround: There is no workaround.

- CSCsl43723

Symptoms: SIP-400 crashed.

Conditions: Occurs after repeated provision/unprovision of ML bundle.

Workaround: There is no workaround.

- CSCsl43735

Symptom: 1. Multiple OI and OQ information which are same for an (S, G) mroute (MGID) on conga.

Conditions: 1. An E3 card with Multicast output interfaces configured.

2. Colliding sources for same multicast group (S1, G) and (S2, G) for above output interfaces.

3. No Egress QoS in the above interfaces.

Workaround: 1. reload the E3 LC 2. do not have colliding sources for multicast.

- CSCsl47221

Symptoms: Traffic may stop because of spurious memory access.

Conditions: Occurs after shutting the qinq subinterface

Workaround: Perform a **shut/no shut** on the subinterface.

- CSCsl47637

Symptoms: Cisco 12000-SIP-401 with SPA-8X1FE-TX-V2 stops forwarding traffic.

Conditions: Occurs on Cisco 12000 routers running the c12kprp-k4p-mz.120-32.SY2g image and with 12000-SIP-401 and SPA-8X1FE-TX-V2. Another three shared port adapters (SPA) were also present. Possibly triggered by multicast traffic.

Workaround: Only a reload of the card/SPA solves the problem.

- CSCsl50271

Symptoms: An Open Shortest Path First (OSPF) enhancement, to avoid a suspend when link state update packets are sent, may result in a router crash.

Conditions: The symptoms are observed in a scenario with 3k tunnels. Both unconfiguring the loopback interface and deleting the loopback interface trigger the same code path that may lead to OSPF suspension.

Workaround: There is no workaround

Further Problem Description: The problem actually exists in all branches. However, this is a timing issue.

- CSCsl51587

Symptoms: The channelized SPA is in admin down state. When the **show hw-module subslot x brief** command is entered on the LC, the LC may crash.

Conditions: Unknown at this time.

Workaround: There is no workaround.

- CSCs151615
Symptoms: Channelized shared port adapter (SPA) out of service after active RP crash.
Conditions: Occurs because of heartbeat failure
Workaround: Reload the SPAs.
- CSCs153811
Symptoms: Some FRR database entries become active after reoptimization. Traffic on the LSP which become FRR active is forwarded to the wrong path and continues to drop.
Conditions: This problem may happen when manual or timer reoptimization is performed during convergence. This problem may happen when "Tunnel head end item" and "LSP midpoint item" in FRR database have more than one entry in each item. This problem may happen when midpoint entry in "LSP midpoint item" is the LSP using "loose" path-option on a headend router.
Workaround: There is no workaround.
Further Problem Description: FRR database state and the traffic recover by doing primary tunnel or backup tunnel's "shutdown" / "no shutdown" if this problem occur. If we configure longer reoptimization timer or we perform manual reoptimization after convergence, this problem may not occur
- CSCs160370
Symptoms: GSR not soaking SLOS and bringing down interface immediately
Conditions: The issue occurs only when the GSR redundancy switchover happens.
Workaround: There is no workaround.
- CSCs162276
*Some packet flows dropped in nexthop load-sharing between TAG and IP
- CSCs163038
Symptoms: Provider edge (PE) not learning MAC addresses as expected.
Conditions: Occurs with Virtual Private LAN Services (VPLS) setup with three PEs.
Workaround: There is no workaround.
- CSCs163885
Symptoms: Packet drops occur when doing MPLS ip2tag and tag2ip load balancing on an Engine 2 line card.
Condition: Occurs on a Cisco 12000 series router running Cisco IOS Release 12.0(32)sy2d.
Workaround: Enable LDP on the the tunnel.
- CSCs165264
Symptoms: EF CAR value does not set properly in TCAM for MFR bundle interface.
Conditions: Occurs when MFR interface is shut and no shut.
Workaround: Remove and re-apply output service policy to the MFR interface.
- CSCs165977
Symptoms: IOS field diagnostics is failing with various error messages about "Slave Clock" such as displayed below:
Error disabling LC Enable register on CSC 0, SCA768_LC_ENABLE_2_S 0x7f, read_count 100 ...
Timed out waiting for TX Network Interrupt to happen ... Slot 16, Slave Clock Control Register 0x00000000

Conditions: This has only been observed on a Cisco 12000 router when there are 12010E-CSC and 12010E-SFC fabric card in the chassis.

Workaround: There is no workaround.

- CSCsl67149

Symptoms: A sync issue is observed with the standby and active configuration.

Conditions: This symptom is observed on a Cisco 12000 series router that is configured for MLPP/MFR. When an attempt is made to remove and add the members before the unprovisioning is completed, the member is added in standby but not in active; hence the configuration sync issue.

Workaround: Add the member after the unprovisioning is completed.

- CSCsl67815

Symptoms: When core-facing line card reloads or has link flap, the edge-facing E3/E5 for mVPN may not forward mVPN traffic.

Conditions: This defect is observed with an internal version off Cisco IOS Release 12.0(33)S.

Workaround: Enter the **clear ip mds line** *<edge facing E5 lc slot>* command.

- CSCsl74425

Symptoms: Engine 5 card crashed following provision/unprovision.

Conditions: Occurs after repeated provision/unprovision of Multilink Point-to-Point Protocol (MLPPP).

Workaround: There is no workaround.

- CSCsl74820

Symptoms: Standby RP crashed.

Conditions: Occurred after provision/unprovision of Multilink Frame Relay (MLFR) MLFR with Hierarchical Quality of Service (HQoS).

Workaround: There is no workaround.

- CSCsl77158

Symptoms: A Cisco router may see the following errors: Oct 30 16:42:04.094 GMT: %ALIGN-3-SPURIOUS: Spurious memory access made at 0x405039FC reading 0x1678

Conditions: The symptoms may be observed on a CISCO7513 running Cisco IOS release 12.0(32)S3 with PA-MC-E3 cards installed.

Workaround: There is no workaround. This problem is not service impacting.

- CSCsl81258

Symptoms: On a Cisco 12000 router running Cisco IOS Release 12.0(32)SY4, the SNMP ifIndex is missing for subinterfaces of the first SPA of a Engine 5 SIP-600 Line Card, as follows:

```
router#sh snmp mib ifmib ifindex GigabitEthernet15/0/3.951 Invalid ifIndex for
GigabitEthernet15/0/3.951
```

This issue affects accounting and billing.

Conditions: Occurred after router was upgraded from Cisco IOS Release 12.0.(31)s6 to Cisco IOS Release 12.0.(32)SY4.

Workaround: There is no workaround.

- CSCsl82857

Symptoms: RP crashes after successful switchover.

Conditions: Occurs when Data-Link Connection Identifiers (DLCI) are deleted from Multilink Frame Relay (MFR) interface, followed by a switchover.

Workaround: There is no workaround.

- CSCs187418

Symptoms: The process IPC Seat Manager is permanently holding a CPU utilization of 40-50%. Causes a considerable decrease in traffic and very slow response from the routers.

Condition: This behavior has been observed on several Cisco 12000 routers with PRP-1 running Cisco IOS Release 12.0(32)SY4 and is conditioned to the following factors: - Several hundreds of interfaces configured like channelized, multilink or virtual template interfaces. Every physical and each of these interfaces has an HWIDB associated with it. - many linecards in the chassis. - The **ip multicast-routing distributed** command is enabled.

Workaround: Upgrade to PRP-2 and CPU would go down to 10-15% in this same process. Or if feasible, disable **ip multicast-routing distributed**.

- CSCs189425

Symptoms: Bidirectional Forwarding Detection (BFD) sessions do not scale. This symptom is especially visible with an OSPF client when one of the peers is rebooted after configuring the maximum number of BFD sessions.

Conditions: This symptom occurs when configuring maximum BFD sessions or total number of BFD sessions too close to the maximum limit.

Workaround: Configure 90 percent of the maximum allowed BFD sessions.

- CSCs192482

Symptoms: Fragmentation is handled incorrectly on GSR E5 line card. We can send up to around 2Gbps of fragmented traffic without performance impact. When the egress line card CPU reaches 100%, the rate of the fragmented traffic drops down to 50Mbps.

Conditions: Occurs when all CPU resources of the egress LC are consumed.

Workaround: There is no workaround.

- CSCs193596

Symptoms: When the MTU is changed on the core-facing E0 LC, all the E0 cards in the router crash.

Conditions: This symptom is observed with bidirectional traffic with an L3VPN, L2VPN configuration. There are also MPLS TE tunnels.

Workaround: There is no workaround.

- CSCs193926

Symptoms: E5 line card configured for CFI and BFI may crash when passing mVPN traffic.

Conditions: This is observed with Cisco IOS Release 12.0(32)SY5.

Workaround: There is no workaround.

- CSCs194410

Symptom: CPU hog condition occurs because of stressful BGP configuration.

Conditions: Occurs in Cisco IOS releases in which CSCsj17879.

Workaround: None

- CSCs194784

Symptoms: Packet drops on output service policy after port swap in Tx BMA of E3 Card. The problem is due to the port-burst being changed incorrectly without any real configuration change on the concerned sub-interfaces.

Conditions: When a Port-swap in Tx BMA is accompanied by the change in burst value after removing service policy (or sub-interface), we are able to see the traffic drop to another sub-interface.

Workaround: Remove and re-add the output service policy from the affected sub-interface.

- CSCsl96577

Symptoms: The **show ppp multilink** statistics are not updated on a Cisco 7500 router.

Conditions: This symptom is observed when dLFIoLL+SSO is configured on the Cisco 7500 router and a switchover is performed.

Workaround: There is no workaround.

- CSCsl98882

Symptoms: Traffic stops forwarding after the deletion of a security output ACL which is shared with the other port on a two-port OC-192, with the port carrying the traffic having a feature-output ACL.

Conditions: Occurs on a two-port OC-192 E6 card. Both the ports should be configured with output or input security ACLs, and one port which is carrying the traffic should have output or input ACL. For this issue to happen, all the ACLs need to be either output or input type simultaneously.

Workaround: Configure a new ACL with a different name from the original ACL, then remove it. The traffic can then be forwarded again.

Further Problem Description: This issue is specific to E6 alone and will not happen on E4.

- CSCsm02749

Symptoms: When multicast VPN routing/forwarding instance (mVRF) is un-configured, memory leak may occur in line cards.

Conditions: This symptom is observed in Cisco 12000 Series Routers and Cisco 7500 Series Routers when multicast distributed routing is enabled on VPN routing/forwarding instance.

Workaround: There is no workaround.

- CSCsm04631

Symptoms: RP crashes due to memory corruption.

Conditions: LC or SPA sending wrong VC number during stats update.

Workaround: There is no workaround.

- CSCsm07692

Symptoms: A SIP600 crashes.

Conditions: When the primary CSC is shut, the SIP600 crashes.

Workaround: There is no workaround.

- CSCsm09927

Symptoms: Interface flaps continuously after running atlas BERT.

Conditions: During atlas BERT another interface with lower anyphy number should be deleted.

Workaround: Reload the shared port adapter (SPA).

- CSCsm10560

Symptoms: A standby route processor crashes with a traceback when multilink is provisioned/unprovisioned continuously.

Conditions: This symptom is observed with a script. There is a small but significant chance of encountering this symptom during manual testing. This symptom occurs in branches based on Cisco IOS Release 12.0S ONLY.

Workaround: There is no workaround.

- CSCsm11787

Symptoms: Customer reporting intermittent loss of L2 tunnel with no error messages.

Conditions: Occurs on a Cisco 7500 router running Cisco IOS Release 12.0(31)S02y.

Workaround: There is no workaround.

- CSCsm12723

Symptoms: Layer 2 Virtual Private Network (L2VPN) CoS (Class of Service) queue becomes unallocated via the **show policy-map int <> dlci <> output** command after a L3VPN subinterface with another policy-map is applied to the same interface.

Conditions: Occurs when both L2vpn and L3vpn under the same interface with different policy-map on both of them.

Workaround: Delete and redefine the layer 2 QoS policy to the Data-Link Connection Identifier (DLCI).

- CSCsm17391

Symptoms: Some Intermediate System-to-Intermediate System (IS-IS) routes are missing in the routing table.

Conditions: This occurs when some interfaces flap.

Workaround: There is no workaround.

- CSCsm24189

Symptoms: 1choc12 ISE: PLIM might reset due to heartbeat failure.

Conditions: This happens when the following errors occur on the PLIM console: [2]T1:5 rx error(crc or non-integer size) 5 [2]T1:5 rx error(crc or non-integer size) 5

And when one or more paths have PAIS.

Workaround: Reduce the TEMUX logging level to 0 as follows **attach slot# plim logctl /dev/temux 0** And then clear the path AIS.

- CSCsm26130

Symptoms: When removing a subinterface from the configuration that contains an IP address that falls into the major net of the static route, the static route is no longer injected into the BGP table. Since the route is not in the BGP table, it is not advertised to any peers.

Conditions: This symptom is observed with auto-summary enabled in BGP. A static summary route is configured to null0 and is injected into the BGP table with a network statement.

Workaround: There are four possible workarounds:

1) Use an "aggregate-address" configuration instead of the static route to generate the summary. 2) Remove auto-summary from the BGP process. 3) Enter the **clear ip bgp *** command. 4) Remove and reconfigure the BGP network statement for the summary route.

- CSCsm32438

Symptoms: The ifStackStatus results for SPA-4XCT3/DS0 on GSR intermittently do not show relationship between Serial interface and T1, nor T1 to CT3.

Conditions: Occurs when running Cisco IOS Release 12.0(32)S6d with SPA-4XCT3/DS0. Polling ifStackStatus results do show layered relationship with Serial interface, T1 to CT3.

Workaround: Remove and add again the T1 link channel-group if possible.

- CSCsm33743

Symptoms: VIP reloads.

Conditions: The crash is triggered by an illegal memory access operation. The issue can affect any interface and on any platform.

Workaround: No workaround.

Further Problem Description: This bug does not impact Cisco IOS Release 12.2SXF, 12.4, or 12.4T releases. This is seen very rarely and is not reproducible in lab.

- CSCsm36057

Symptoms: "Warning: error msgs in vc stats" messages are displayed continuously on the console.

Conditions: This symptom is observed when the router is reloaded.

Workaround: There is no workaround.

If any statistics are not being updated properly on the serial interfaces on the Ch-SPAs, enable the **debug hw sub slot/bay** command on the RP.

- CSCsm41303

Symptoms: A Cisco 12000 router with SIP-601 linecards may experience high CPU in the Tag Input process because of many packets being punted by the linecards to the PRP CPU. The packets are MPLS TTL expired packets that require an unreachable to be sent back. These packets should be processed on the linecard, but they are not.

Conditions: This symptom is observed only on SIP-601 10G linecards.

Workaround: There is no workaround.

- CSCsm43195

Symptoms: A configuration of L2VPN interworking between SIP-601/GE SPA to SIP-401/CT3/FR DLCI switching and with a QoS egress policy applied on the SIP-601 GE SPA interface, traffic may propagate egress on the GE port.

Conditions: When the policy is not applied, traffic flows egress on the GE SPA based interface. When the policy is applied, no traffic is seen egress on the GE interfaces.

Workaround: There is no workaround.

- CSCsm44620

Symptoms: Multicast tunnel not coming up after RPM change. A misconfiguration with overlapping networks causes the join to be rejected. This can be seen on the PIM neighbor list.

Conditions: There is a problem related to one of the hub card in rpm-xf.10 in forwarding PIM traffic from 2 PEs (rpm-xf.13 & rpm-xf.11). After RP migration from AVICI to CRS we found that tunnels from PE in slot 13 were not coming up. PE in slot 13 was in consistently in registering mode. PE was not coming out of registering mode which was preventing the tunnels from coming up. For PE to come out of registering mode S,G state should be built from new RP down to PE. At this stage the CRS (RP) showed that S,G tree was establish at the RP. S,G tree was OK all the way down from CRS to the last hop (P in slot 10) connecting to the slot 13 PE. The P router in slot 10, which is directly connected to PE, showed that S,G state was established and PE facing interface was in OIL.

But there were couple of discrepancies on the P in slot 10. There were no flags set on this P for the mroute of PE. In addition, we found that PE was not receiving any PIM traffic from the P in slot 10. This led to suspicion that although the P showed the correct S,G and OIL but is still not able to forward traffic to the PE. And this could be the reason for PE to remain in registering mode hence preventing the tunnels from coming up.

Workaround: Remove the following configurations:

a. rpm-xfh10-z135 - shut & remove interface Switch1.4073 b. rpm-xfh09-z134 - shut & remove interface Switch1.4073 c. rpm-xfp11-1172 - remove interface Switch1.3172 d. rpm-xfp13-z074 - remove interface Switch1.4074 e. rpm-xfp04-1171 - remove interface Switch1.3171

- CSCsm45113

Symptom: Router may install duplicate routes or incorrect route netmask into routing table. It could happen on any routing protocol. Additionally, for OSPF, crash was observed.

Conditions: The problem is triggered by SNMP polling of ipRouteTable MIB. The problem is introduced by CSCsj50773, see the Integrated-in field of CSCsj50773 for affected images.

Workaround: Do not poll ipRouteTable MIB, poll newer replacement ipForward MIB. instead. The ipRouteTable MIB was replaced by ipForward MIB in RFC 1354.

Further problem description: The **clear ip route *** command can correct the routing table until the next poll of ipRouteTable MIB.

- CSCsm45311

Symptoms: Active RP crashes because of FIA error.

Conditions: Crash is seen when ML provisioning/unprovisioning and Buffer Recarve is done.

Workaround: There is no workaround.

- CSCsm45666

Symptoms: E5 LC crash on startup with multicast traffic flowing.

Conditions: Reboot the router.

Workaround: There is no workaround.

- CSCsm48176

Symptoms: Line cards on a Cisco 12000 series router or a Cisco 7500 router might crash.

Conditions: This symptom is observed when the **no ip multicast- routing distributed** command for a VRF is issued when multicast tunnels are up. This symptom is also observed when MVRFs are deleted.

Workaround: Stop multicast traffic before deleting VRFs or issuing the **no ip multicast-routing distributed** command.

- CSCsm55274

Symptoms: Class Based Tunnel Selection (CBTS) stops working. Packets are sent through the wrong tunnel.

Conditions: This symptom is observed when the tunnel flaps.

Workaround: There is no workaround. Once CBTS is broken, only a reload of the Line card clears the problem.

- CSCsm57369

Symptoms: On switchover, we see the overhead message appearing in config if we have not configured.

Conditions: This symptom is observed only if there is a switchover in RPR+ or SSO mode.

Workaround: Manually change the config to restore the previous config.

- CSCsm62033

Symptoms: L2TP session does not come up.

Conditions: Occurs when a Cisco router marks the Call Serial Number AVP in the ICRP as mandatory. This causes a third-party router to reject it.

Workaround: There is no workaround.

- CSCsm64491

Symptoms: Connecting SPA-4XCT3/DS0 SPAs back to back and executing the **hw-module subslot x/y reload** command causes the line card to crash.

Conditions: All the interfaces should be up and running. Note that this symptom occurs only because of the issue introduced by CSCsg96660; it is not seen otherwise without the image having the fix for CSCsg96660.

Workaround: There is no workaround.

- CSCsm66081

Symptoms: If a multilink interface has one end connected to a Cisco 12000 router with a CHOC12/DS1-IR-SC and the other end connected to a non-Cisco- 12000 router, then the multilink interface receiver, at the non-Cisco-12000 router side, may drop all received packets because of packet fragment loss or out-of-order.

Conditions: This symptom may occur immediately when the first member link comes back up again after all member links of the multilink interface have gone down.

Workaround:

1) Create a new multilink interface.

2) Move the member links from the current multilink interface to the new multilink interface.

- CSCsm66635

Symptoms: E5 BF/CFI on same line card, PIM-DM traffic may not flow for CFI or Auto-RP information may also not flow. So far the problem is identified to be in E5 BFI/CFI card which drops the DM data packets instead of punting them which is needed for the (*,G)/(S,G) state creation and packet flooding for DM to work.

Conditions: This defect is observed with Cisco IOS Release 12.0(32)SY5.

Workaround: Use the **clear ip mds line** command on the E5 and core line cards to solve the problem.

- CSCsm70668

Symptoms: A soft OIR over E3:POS impacts complete traffic with a biscuit tunnel.

Condition: A soft OIR over E3:POS impacts complete traffic with a biscuit tunnel configured. In OIR "test mbus power 6 off" and "test mbus power 6 on" are performed followed by a microcode reload on slot 6.

Workaround: There is no workaround.

- CSCsm71063

Symptoms: The **shape fecn-adapt** command is accepted in the configuration, but it is not shown in output from **show running-config** or **show policy-map**.

Conditions: When **shape fecn-adapt** is configured with shaping configured on the serial interface with frame-relay, **show policy-map** does not show the **shape fecn-adapt** being configured. The **show policy-map int** command shows **fecn-adapt** as "0".

Workaround: There is no workaround.

- CSCsm74769

Symptoms: if_num mismatch is seen in the uidb, sometimes along with the L2TPv3 bit set to zero. As a result, customer saw L2TPv3 packet drops over FR in Cisco 12000 series Internet router.

Conditions: Removing xconnect on remote PE, resulting in a session(DLCI) FLAP on the local PE. Trigger is L2TPv3 session flap; this may cause a stale CI->Udb mapping in internal data-structures resulting in if-num mismatch in uidb if the old CI is reused by an DLCI on a different interface.

Workaround: Reload the affected line card.

- CSCsm75339

Symptoms: Tracebacks on mic-reload of SIP601.

Conditions: Mic-reload of SIP601 with CT3 SPA.

Workaround: Reloading the secondary RP should restore the out-of-sync ifindex tables.

- CSCsm82260

*Some packet flows dropped in nexthop load-sharing between TAG and IP

- CSCsm82600

Symptoms: PRP-1 fails to boot after an OIR/power cycle. LEDs might show RPT SENT or RP RDY.

Conditions: This symptom is observed upon a power cycle after upgrading the mbus-agent-rom of the PRP.

Workaround: Use the upgrade mbus-agent-rom slot force command with an older version of Cisco IOS software in the active RP to downgrade the mbus agent ROM of the problem RP.

- CSCsm92567

Symptoms: After an RP switchover (SSO), or performing the following procedure, the VPWS DLCI output queues become unallocated.

1. Add VPWS DLCI with service-policy to the FR main interface. 2. Add an FR subinterface but with LFI enabled. 3. Bounce the service policy class on the DLCI under the main interface.

Conditions: When a VPWS circuit is configured on the FR main interface and L3 subinterface has LFI enabled. QoS is applied to both L2VPN and L3VPN services.

Workaround:

1. Delete the LFI FR service-policy. 2. Bounce QoS again on the VPWS DLCI.

- CSCso01440

Symptoms: PE1 2/2/1 <-----> 4/0/1CE1

Connect SPA-4XCT3/DS0 SPA back to back, configure loopback network at CE1, and then run bert on 4 T1 channels in PE1. After this, bert will not stop even though the time interval elapsed.

Conditions: All the interfaces should be up and running.

Workaround: There is no workaround.

- CSCso12748

Symptoms: Tunnels between Cisco and non Cisco peers fail to come up since the Mandatory of Message Type AVP for SCCRQ that is sent by Cisco is FALSE.

Conditions: This symptom occurs because the Mandatory of Message Type AVP for SCCRQ that is sent by Cisco is FALSE.

Workaround: There is no workaround.

- CSCso19528

Symptoms: Traffic may not flow after a switchover.

Conditions: The symptom may be observed when dLFioLL + HA is configured on a Cisco 7500 router.

Workaround: Wait for standby to come up.

- CSCso19748

Symptoms: An 80-byte buffer depletion occurs on E5, leading to an outage of all serial links.

Conditions: The conditions under which this symptom is observed are unknown.

Workaround: There is no workaround.

- CSCso21681

Symptoms: An output policy on an MFR interface disappears when the SIP 601 card is reset.

Conditions: Configure the service policy and apply it to the output of the MFR interface. Reset the SIP 601 card, and the service policy will disappear from configuration.

Workaround: There is no workaround.

- CSCso22098

Symptoms: OSPF neighborhood goes down on RPR+ switchover on core router. The router does not send any hello packets to the connected routers.

Conditions: Occurs when executing RPR or RPR+ switchover. No Problem seen with SSO switchover.

Workaround: There is no workaround.

- CSCso22730

Symptoms: Prefixes learned via IGP (ISIS) get assigned "imp-null" as the local label for them.

Conditions: The router has ECMP paths to uplink routers via POS interfaces. It runs ISIS as an IGP. There could be TE tunnel configured on the POS interface. And frequent interface flaps.

Workaround: There is no workaround. Clear the route or flap the interface to bring back the correct local label.

- CSCso25026

Symptoms: SONET Section Data Communications Channel (SDCC) comes up initially and goes down after some time and never comes up again. The interface shows up, but the line protocol shows down on both the sides

Conditions: Occurs after packet over SONET (POS) is converted to spatial reuse protocol (SRP).

Workaround: There is no workaround.

- CSCso25848

Symptoms: With an ingress E2 GigE line card and an egress E5 line card, packets are dropped in the egress line card with TX bad BMA buffer counts increasing.

Conditions: This symptom is observed when the ingress is E2 and the egress is E5.

Workaround: There is no workaround.

Further Problem Description: This issue is not seen with an E3/E5 combination or an E2/E6 combination.

- CSCso30471

Symptoms: Engine 5 SIP-600 crashes and tracebacks seen for Flexible NetFlow (FNF) configuration.

Conditions: Line card crash is hard to reproduce, and it is seen when **show flow monitor** is used. Tracebacks are easily re-producible while unconfiguring FNF output mode.

Workaround: There is no workaround.

- CSCso31508

Symptoms: CEF and hardware CEF for global default route are inconsistent. This may cause the default traffic to be sent through the wrong interface.

Conditions: This issue occurs under the following conditions:

1. Global default should point toward the core. 2. VRF default should be learned from the remote PE.

Workaround: Enter the following command:

clear ip route 0.0.0.0 0.0.0.0

- CSCso33290

Symptoms: L2VPN traffic on an MFR interface is unable to pass through FR/IETF encapsulation MPLS trunk. Furthermore, if this MFR interface is deleted and re-added, the following error messages are received.

SLOT 4:Mar 20 11:51:05.459 UTC: %SPA_CHOC_DSX-3-ERROR: Serial4/0/0/1:0: response parsing failed for DLCI (601) provisioning
SLOT 4:Mar 20 11:51:05.471 UTC: %SPA_CHOC_DSX-3-ERROR: Serial4/0/0/1:0: response parsing failed for DLCI (602) provisioning

Conditions: This symptom is observed after an MFR interface is deleted and re-added.

Workaround: There is no workaround.

- CSCso46965

Symptoms: Ping fails

Conditions: Occurs when 2x1GE V2 shared port adapter (SPA) is in BN jacket.

Workaround: There is no workaround.

- CSCso47485

Symptoms: The E4+ line card crashes continuously with the following output:

SLOT 1:Jan 19 02:06:09.559 UTC: %TX192-3-CPUIF: Error=0x40
rd 0x15 base 0x12 hdr 0x14 last 0x14 wr 0x14 insert 0x0 back 0x1 len 0x2474 cnt 0x0

Conditions: There is no exact trigger. But this symptom is observed when there are corrupt packets being sent from the ingress card under unknown circumstances.

Workaround: There is no workaround.

- CSCso53048

Symptoms: A router acting as an OSPF ABR for an NSSA area, when announcing a default route into the NSSA area, sets the LSA forwarding address to one of its interfaces instead of to 0.0.0.0. When there is more than one interface from that router into the NSSA area (load balancing), only

one interface will be used by NSSA routers to forward traffic toward destinations reachable via the default route. If there is no default route present in the RIB, the forwarding address is set to 0.0.0.0, which will enable load balancing.

Conditions: This behavior is not present in Cisco IOS Release 12.0(32)SY4.

Workaround: To have load balancing, you may want to define a loopback inside the NSSA to be elected as the FA and have the FA visible from the interfaces into the NSSA.

- CSCso60329

Symptoms: With L3VPN config over IP using L2TPV3 tunnel configuration, the input queues of interface is wedged. The **show buffer input interface** command yields no output.

Conditions: Occurs with the configuration of L3VPN over IP using L2TPV3 tunnels.

Workaround: There is no workaround.

- CSCso82147

Symptoms: Line card crashes when packet over SONET (POS) shared port adapter (SPA) is present.

Conditions: Occurs the first time router is reloaded.

Workaround: There is no workaround.

- CSCso86881

Symptoms: Per-Packet Load Balancing (PPLB) does not work and traffic goes through single interface.

Conditions: Observed in following case: * CE1---PE----CE2. * Two links from CE1 to provider edge (PE) and two links from PE to CE2. * All the four links are emerging from same shared port adapter (SPA) on PE. * Serial interface is used. * VPN routing/forwarding (VRF) is configured on PE.

Workaround: Remove PPLB and configure it back. However, the issue will reappear on router or line card reload.

- CSCso89193

None Symptom:

c7200-kboot-mz image is broken by the commit of CSCso71150

Workaround:

No workaround

- CSCso92950

Symptoms: IPv6 multicast unnecessarily copied when join -> prune is repeated multiple times.

Conditions: Occurs when IPv6 multicast-routing is enabled on a Cisco 12000 series router.

Workaround: Reload the router.

- CSCsq00167

Symptoms: 12000-SIP-401/501/601 has 8 MB of FSRAM with the fix CSCsm13564. But PLU and TLU adjacencies in the 12000-SIP-401/501/601 support up to 4 MB.

Conditions: If the hardware is supporting 8 MB of FSRAM, the PLU can have access to this 8 MB. But this is not happening.

Workaround: Identified through the code review of CSCsm13564. There is no workaround.

- CSCsq00596

Symptoms: CE-CE ping is not working in Frame Relay over MPLS (FRoMPLS).

Condition: Occurs when E0 POS is used as disposition.

Workaround: There is no workaround.

- CSCsq02587

Symptoms: Traffic engineering (TE) tunnel is not coming up in MPLS TE.

Condition: Occurs when both Ethernet Over MPLS (EoMPLS) and MPLS TE are configured on the router.

Workaround: There is no workaround.

- CSCsq03170

Symptoms: An input service policy with only the class-default class shows no matches.

Conditions: This symptom is observed after a reload of Cisco 12000 series routers, Linecard Engine 3, with an ATM interface configured for AToM, Port Mode.

Workaround: Move traffic and the configuration to another interface.

- CSCsq04787

Symptoms: Router crashed when issuing the **show-tech** command while connected to the router using SSH.

Conditions: Occurred on a Cisco 7200 router with NPE-G2 running Cisco IOS Release 12.0(33)S.

Workaround: Use telnet to connect to the router.

- CSCsq05128

Symptoms: Performance Route Processor (PRP) crashes after loading image from disk0.

Condition: Occurs when multiservice edge (MSE) router reloads with the image in the disk0. The RP crashes, and tracebacks are displayed. Both the active and standby RPs toggle each time.

Workaround: There is no workaround.

- CSCsq05602

Symptoms: Intermediate System-to-Intermediate System (IS-IS) routes still using MPLS tunnels as next hop even after tunnels are shutdown.

Conditions: Occurs when MPLS tunnels to multiple routers are configured.

Workaround: Use the **clear isis *** command to temporarily solve the problem.

- CSCsq16042

Symptoms: The OSPF state of interfaces on a Cisco 7500 RSP router will stay down after a reload or when the interface are brought down and then up.

Conditions: This only affects Cisco 7500 RSP routers.

Workaround: There is no workaround.

- CSCsq26219

*Some packet flows dropped in nexthop load-sharing between TAG and IP

- CSCsq70534

Symptoms: A router crashes because of a block overrun (overwriting the memory block).

Conditions: This symptom is observed only when templates are exported in the export packet, which is used only in version 9 version of exporting.

Workaround: Version 5 could be used for exporting.

- CSCsq85868

Symptoms: Performance Route Processor (PRP) crashes after loading image from disk0.

Condition: Occurs when multiservice edge (MSE) router reloads with the image in the disk0. The RP crashes, and tracebacks are displayed. Both the active and standby RPs toggle each time.

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.0(33)S

All the caveats listed in this section are resolved in Cisco IOS Release 12.0(33)S. This section describes only severity 1, severity 2, and select severity 3 caveats.

ISO CLNS

- CSCsh63785

Symptoms: A MPLS tunnel may not come up after a stateful switchover (SSO) has occurred.

Conditions: This symptom is observed on a Cisco router when Cisco IS-IS NSF is enabled and when IS-IS is used as the IGP for MPLS TE tunnels.

Workaround: Do not configure Cisco IS-IS NSF. Rather, configure IETF NSF.

First Alternate Workaround: Enter the **clear isis *** command.

Second Alternate Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface that is used for the MPLS TE tunnels after the SSO has occurred.

Miscellaneous

- CSCec12299

Devices running Cisco IOS versions 12.0S, 12.2, 12.3 or 12.4 and configured for Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) or VPN Routing and Forwarding Lite (VRF Lite) and using Border Gateway Protocol (BGP) between Customer Edge (CE) and Provider Edge (PE) devices may permit information to propagate between VPNs.

Workarounds are available to help mitigate this vulnerability.

This issue is triggered by a logic error when processing extended communities on the PE device.

This issue cannot be deterministically exploited by an attacker.

Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080924-vpn.shtml>.

- CSCek61276

Symptoms: IPv6 traffic stops.

Conditions: This symptom is observed on a Cisco router when you first disable and then re-enable IPv6 on an interface.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface.

- CSCsc53393
Symptoms: A Cisco 12000 series may generate the following error message and reload unexpectedly because of a bus error:
%MEM_ECC-2-MBE: Multiple bit error detected at XXXXXXXX:
%MEM_ECC-3-SYNDROME_MBE: 8-bit Syndrome for the detected Multi-bit error: 0x99
Conditions: This symptom is observed on a Cisco 12000 series that is configured for CEF and MPLS.
Workaround: There is no workaround.
- CSCsd20210
Symptoms: The PXF engine of a Cisco 10720 may crash.
Conditions: The symptom is observed when you modify an existing access control list (ACL) that is attached to an interface.
Workaround: Do not modify an ACL that is attached to an interface. If you cannot remove the ACL from the interface, create a new ACL and apply it to the interface.
- CSCsg61922
Symptoms: The **show l2tp session all vcid** command generates incorrect output.
Conditions: This symptom is observed on a Cisco router that has an L2TPv3 tunnel.
Workaround: There is no workaround.
- CSCsg70932
Symptoms: A Cisco 7200 series that is configured for QoS may crash when traffic is sent.
Conditions: This symptom is observed on a Cisco 7200 series that has an NPE-G1 or NPE-G2 and that has a Port Adapter Jacket Card in which a 2-port OC-3/STM-1 POS port adapter (PA-POS-2OC3) is installed that has an interface with a service policy.
Workaround: There is no workaround.
- CSCsj25476
Symptoms: Route processor crashes.
Conditions: Occurs while executing the command **no control-plane slot <slot no>** command.
Workaround: There is no workaround.
- CSCsk47914
Symptoms: Traffic forwarding stops upon mic-reloading the egress card when E4+ is ingress.
Conditions: Occurs when mic-reloading the egress line card
Workaround: Mic-reload the E4+ line card to recover. You can also enter the **clear cef linecard <ingress card slot#>** command to recover traffic.
- CSCsk67111
Symptoms: Watchdog timeout occurs after switchover.
Conditions: Occurs when the high-availability feature is configured on the RPR of a Cisco 7500 router.
Workaround: There is no workaround.
- CSCsl09865
Symptoms: Memory leak occurs on Cisco 10720 router.

Conditions: Occurs when the router receives a “pim join” message. The router allocates blocks of memory that are never released. Occurs when there are more than three IPv6 PIM hosts on the same network segment.

Workaround: There is no workaround.

- CSCsl33781

Symptoms: Primary RP crashes when the **clear counter** command is entered.

Conditions: Occurs when the command is issued while traffic is flowing.

Workaround: There is no workaround.

- CSCsl34355

Two crafted Protocol Independent Multicast (PIM) packet vulnerabilities exist in Cisco IOS software that may lead to a denial of service (DoS) condition. Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20080924-multicast.shtml>.

Open Caveats—Cisco IOS Release 12.0(33)S

This section describes possibly unexpected behavior by Cisco IOS Release 12.0(33)S. All the caveats listed in this section are open in Cisco IOS Release 12.0(33)S. This section describes only severity 1, severity 2, and select severity 3 caveats.

IP Routing Protocols

- CSCek77029

Symptoms: The **remove-private-as** command does not work as expected when applied to a neighbor for which a route-map with a “set as-path prepend” and “continue” statement are configured.

Conditions: Occurred on a router with the following configuration:

```
route-map test permit 10
set as-path prepend 2
continue
route-map test permit 20
set metric 200
```

Workaround: Do not use the **remove-private-as** command with the above configuration.

- CSCsb63652

Symptoms: BGP convergence is very slow and CPU utilization at BGP Router process is always near 100% during the convergence at aggregation router.

Conditions: Occurs if the number of component prefixes belonging to the aggregate-address entry increases. Also occurs if the number of duplicate aggregation component prefixes for aggregate-address entry increases

Workaround: Remove the “aggregate-address” statement.

- CSCsc27668

Symptoms: When you enter the **neighbor ip address send-label explicit-null** command, the RP may crash.

Conditions: This symptom is observed on a Cisco router that is configured for BGP.

Workaround: There is no workaround.

- CSCsd54539

Symptoms: After the command **route-map test-comm-in permit 20** is issued, one of the peers should be denied and should not be advertised to any other peers. But this behavior is not seen with this image.

Conditions: Occurs when the **route map test-comm-in permit 20** is entered.

Workaround: There is no workaround.

- CSCsg42672

Symptoms: On a Cisco router running Cisco IOS release 12.0(32)S4 and configured with BGP and peer-groups, if the Fast Peering Session Deactivation feature is configured in the peer-group, the router automatically configures on the command a route-map with the same name as the peer-group.

Conditions: Occurs when the following is configured:

```
RR#conf t
Enter configuration commands, one per line. End with CNTL/Z.
RR(config)#router bgp 65001
RR(config-router)#neighbor rrs-client fall-over ?
bfd Use BFD to detect failure
route-map Route map for peer route
<cr>
RR(config-router)#neighbor rrs-client fall-over
RR#sh ru
<snip>
router bgp 65001
neighbor rrs-client peer-group
neighbor rrs-client remote-as 20959
neighbor rrs-client update-source Loopback0
neighbor rrs-client fall-over route-map rrs-client <++++>
the route-map does not exist.
```

Workaround: Configure the neighbor individually or use peer-templates

- CSCsg48540

Symptoms: A carrier supporting carrier (CsC) Multiprotocol Border Gateway Protocol (MPBGP) connection between two PE routers may remain in the active state but never becomes established.

Conditions: This symptom is observed when (CsC) is configured on all routers.

Workaround: There is no workaround.

- CSCsi68795

Symptoms: A PE that is part of a confederation and receives a VPNv4 prefix from an internal and an external confederation peer assigns a local label to the prefix despite the fact that the prefix is not local to this PE and that the PE is not changing the BGP next-hop.

Conditions: Occurs when receiving this prefix via two paths from confederation peers.

Workaround There is no workaround.

Further Problem Description: Whether or not the PE will chose to allocate a local label depends on the order at which the multiple paths for this vpnv4 prefix are learned. The immediate impact is that the local label that is allocated takes up memory in the router as the router will populate the LFIB with the labels.

- CSCsj56281

Symptoms: Inherit peer-policy does not work after a router reload

Conditions: Occurs only after the router is reloaded.

Workaround: There is no workaround.

- CSCsk23478

Symptoms: When converting BGP from NLRI to AF form, route-maps are not applied to the multicast neighbor.

Conditions: Occurs when a neighbor is supporting both unicast and multicast. If a route-map is applied to the neighbor, it will only be applied to the IPv4 unicast address-family after converting with the **bgp upgrade-cli** command

Workaround: If the route-map is needed for the unicast and multicast address-family, then the command **match nlri unicast multicast** should be added to the route-map, even though this is the default behavior.

- CSCsl30331

Symptoms: Prefixes are allowed by the outbound route-map even though the match condition is met and the action is set to deny

1. The iteration with the deny action contains a match community.

2. The continue statement is used in one of the previous iterations.

Workaround: If there is single match clause based on NLRI, the condition is avoided. The issue is not observed.

- CSCuk59727

Symptoms: The output of the **show stacks** command may show a very large number of blank lines (for example, 280,000) instead of a process name before the next line of command output is shown.

Conditions: This symptom is observed on a Cisco 12000 series. The symptom may also occur when you enter a command that executes the **show stacks** command such as the **show tech** command or the **show tech cef** command.

Workaround: There is no workaround.

ISO CLNS

- CSCsk66339

Symptoms: A Cisco 7600 router may encounter a condition such that when IS-IS and Traffic Engineering are configured, IS-IS should remove the native path from its local RIB and call RIB code to remove the path from global RIB but fails by either not passing the “delete” msg to RIB properly or RIB doesn’t react when it received the “delete” call.

Conditions: Output from the **show mpls traffic-engineering tunnel** command may indicate the “Removal Trigger: setup timed out” status.

Workaround: Shut/no shut the interface or change the metric temporarily to force an update by using the **tunnel mpls traffic-eng autoroute metric 1** command.

Miscellaneous

- CSCsg32465

Symptoms: Incorrect police percent conversions occur in the second and third levels of a policy.

Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2SB. However, the symptom is platform-independent.

Workaround: There is no workaround.

- CSCsh28556

Symptoms: When configuring frame relay queueing, bandwidth is taken as 28kbps and more than 28 kbps cannot be configured.

Conditions: This happens only when service policy is applied under map-class frame-relay and then binding it under the DLCI with frame-relay traffic shaping enabled under the interface.

Workaround: There is no workaround.

- CSCsh59300

Symptoms: Standby may crash repeatedly

Conditions: Occur when dLFioLL+QoS+SSO is configured on a Cisco 7500 router. Input service policy is configured on MCT1E1 interface.

Workaround: Change the mode to RPR+

- CSCsh77320

Symptoms: Cisco 7500 router is unable to provide adequate guarantee to classes.

Conditions: Occurs when dLFioLL and QoS are configured on 7500 router

Workaround: There is no workaround.

- CSCsi15007

Symptoms: RIP process uses excessive CPU.

Conditions: Occurs when 200 network commands are configured using RIP version 2.

Workaround: There is no workaround

- CSCsi50772

Symptoms: During setup of vc-class provision for l2tpv3 ATM tunnels, the initial end-to-end is just fine, but after removing vc-class on both PE at the same time by script, one of ATM sub-interface on CE router went down, and ping was not passing through anymore.

Conditions: Occurs when the vc-class on PE1 and PE2 are removed at almost at the same time.

Workaround: Remove vc-class on one PE router first, and then remove vc-class on the other PE router.

- CSCsi53353

Symptoms: IPv6 EBGP sessions fail with the following message in “debug bgp events”:

```
%BGP-4-INCORRECT_TTL: Discarded message with TTL 32 from <ip>
```

Conditions: Occurs when BTSH is configured between the peers.

Workaround: Disable BTSH between the IPv6 peers

- CSCsi90548

Symptoms: Cisco 7206VXR with PA-MC-8TE1+ experiences interface flaps when there is a service policy configured on the interface.

Conditions: Occurs when the configured service policy limit is reached.

Workaround: There is no workaround.

- CSCsi95175

Symptoms: Output for **set-mpls-exp-imposition-transmit** is incorrect.

Conditions: The following is output when the command is entered:

```
75Q2-R3(config)#policy-map multiple_action_1
75Q2-R3(config-pmap)# class 35
75Q2-R3(config-pmap-c)# police cir 8000 bc 1000 pir 10000 be 12000
75Q2-R3(config-pmap-c-police)#conform-action set-mpls-exp-imposition-transmit 5
75Q2-R3#sh policy-map
Policy Map multiple_action_1
Class 35
police cir 8000 bc 1000 pir 10000 be 12000
conform-action set-mpls-exp-transmit 5 <<<should be set-mpls-exp-imposition-transmit 5
exceed-action drop
violate-action drop
Workaround: There is no workaround.
```

- CSCsk68742

Symptoms: Using the **show ip mds stats linecard** command shows MDFS reloads on all LCs when multicast distributed routing is added on a VRF through the configuration of ip **multicast-routing vrf vpn distributed**.

Workaround: There is no workaround.

Further Problem Description:

Note that while the MDFS reload is a real reload, it is without a preceding clear so it will not generally cause traffic interruption as it merely causes the same information to be downloaded to the linecards again. However in a highly scaled system running close to the limit, the additional load introduced by a full MDFS reload of every linecard may cause additional failures because of CPU utilization.

- CSCsk69194

Symptoms: Shape average percent calculation is incorrect.

Conditions: This issue is seen on a Cisco 7500 router configured for dLFIoLL. The policy is attached to ATM and multilink interfaces.

Workaround: there is no workaround.

- CSCsl30246

Symptoms: IP PIM neighbor in multicast VPN is not two-way

Conditions: Occurs in traffic between a Cisco 12000 router and a Cisco 7500 router. The Cisco 7500 does not receive MDT update.

Workaround: There is no workaround.

- CSCsl53811

Symptoms: Some FRR database entries become active after reoptimization. Traffic on the LSP which become FRR active is forwarded wrong path and continues to drop.

Conditions:

- This problem may happen when manual or timer reoptimization is performed during convergence
- This problem may happen when “Tunnel head end item” and “LSP midpoint item” in FRR database have more than one entry in each item.
- This problem may happen when midpoint entry in “LSP midpoint item” is the LSP using “loose” path-option on a headend router.

Workaround: There is no workaround.

- CSCsl63438

Symptoms: The Unicast and Multicast VPN traffic packets are dropped on a MLFR bundle link while increasing the traffic rate and bringing back to normal.

Conditions: The drops are seen only after an increase in the traffic rate and bringing back to normal value.

Workaround: There is no workaround.

- CSCsl64686

Symptoms: VIP with CHSTM1 crashes on a Cisco 7500 router.

Conditions: dLFIoLL is configured on a Cisco 7500 router and MDR reload is done on the VIP

Workaround: There is no workaround.

Wide-Area Networking

- CSCsb64662

This caveat consists of two symptoms, two conditions, and two workarounds:

Symptom 1: Multicast packets that traverse a Frame Relay virtual circuit (VC) bundle are dropped.

Condition 1: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0S.

Workaround 1: There is no workaround.

Symptom 2: Multicast packets that traverse a Frame Relay virtual circuit (VC) bundle are process-switched.

Condition 2: This symptom is observed with Cisco IOS Release 12.3.

Workaround 2: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.0(32)S15

Cisco IOS Release 12.0(32)S15 is a rebuild of Cisco IOS Release 12.0(32)S. The caveats listed in this section are resolved in Cisco IOS Release 12.0(32)S15 but may be open in previous Cisco IOS releases. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCek38939

Symptoms: The input error counter may not be incremented for packet errors such as runts, CRC errors, and overrun errors.

Conditions: This symptom is observed on a Cisco 7200 series that has an NPE-G1 or a Cisco 3800.

Workaround: There is no workaround.

- CSCsu96698

Symptoms: More specific routes are advertised and withdrawn later even if **config aggregate-address net mask summary-only** is configured. The BGP table shows the specific prefixes as suppressed with s>.

Conditions: This occurs only with very large configurations.

Workaround: Configure a distribute-list in BGP process that denies all of the aggregation child routes.

- CSCsz71787

Symptoms: A router crashes when it is configured with DLSw.

Conditions: A vulnerability exists in Cisco IOS software when processing UDP and IP protocol 91 packets. This vulnerability does not affect TCP packet processing. A successful exploitation may result in a reload of the system, leading to a denial of service (DoS) condition.

Cisco IOS devices that are configured for DLSw with the **dlsw local-peer** command automatically listen for IP protocol 91 packets. A Cisco IOS device that is configured for DLSw with the **dlsw local-peer peer-id <IP- address>** command listen for IP protocol 91 packets and UDP port 2067.

Cisco IOS devices listen to IP protocol 91 packets when DLSw is configured. However, it is only used if DLSw is configured for Fast Sequenced Transport (FST). A DLSw FST peer configuration will contain the following line:

```
dlsw remote-peer 0 fst <ip-address>
```

It is possible to disable UDP processing in DLSw with the **dlsw udp-disable** command. However, disabling UDP only prevents the sending of UDP packets; it does not prevent the device from receiving and processing incoming UDP packets.

Workaround: The workaround consists of filtering UDP packets to port 2067 and IP protocol 91 packets. Filters can be applied at network boundaries to filter all IP protocol 91 packets and UDP packets to port 2067, or filters can be applied on individual affected devices to permit such traffic only from trusted peer IP addresses. However, since both of the protocols are connectionless, it is possible for an attacker to spoof malformed packets from legitimate peer IP addresses.

As soon as DLSw is configured, the Cisco IOS device begins listening on IP protocol 91. However, this protocol is used only if DLSw is configured for Fast Sequenced Transport (FST). A DLSw FST peer configuration will contain the following line:

```
dlsw remote-peer 0 fst <ip-address>
```

If FST is used, filtering IP protocol 91 will break the operation, so filters need to permit protocol 91 traffic from legitimate peer IP addresses.

It is possible to disable UDP processing in DLSw with the **dlsw udp-disable** command. However, disabling UDP only prevents the sending of UDP packets; it does not prevent the receiving and processing of incoming UDP packets. To protect a vulnerable device from malicious packets via UDP port 2067, both of the following actions must be taken:

1. Disable UDP outgoing packets with the **dlsw udp-disable** command
2. Filter UDP 2067 in the vulnerable device using infrastructure ACL.

* Using Control Plane Policing on Affected Devices

Control Plane Policing (CoPP) can be used to block untrusted DLSw traffic to the device. Cisco IOS software releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP may be configured on a device to protect the management and control planes to minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic sent to infrastructure devices in accordance with existing security policies and configurations. The following example, which uses 192.168.100.1 to represent a trusted host, can be adapted to your network. If FST is not used, protocol 91 may be completely filtered. Additionally, if UDP is disabled with the **dlsw udp-disable** command, UDP port 2067 may also be completely filtered.

```
!--- Deny DLSw traffic from trusted hosts to all IP addresses
!--- configured on all interfaces of the affected device so that
!--- it will be allowed by the CoPP feature.

access-list 111 deny udp host 192.168.100.1 any eq 2067 access-list 111 deny 91 host
192.168.100.1 any

!--- Permit all other DLSw traffic sent to all IP addresses
!--- configured on all interfaces of the affected device so that it
!--- will be policed and dropped by the CoPP feature.

access-list 111 permit udp any any eq 2067 access-list 111 permit 91 any any

!--- Permit (Police or Drop)/Deny (Allow) all other Layer 3 and Layer 4
!--- traffic in accordance with existing security policies and
!--- configurations for traffic that is authorized to be sent
```

```
!--- to infrastructure devices.
!--- Create a Class-Map for traffic to be policed by
!--- the CoPP feature.

class-map match-all drop-DLSw-class match access-group 111
!--- Create a Policy-Map that will be applied to the
!--- Control-Plane of the device.

policy-map drop-DLSw-traffic class drop-DLSw-class drop
!--- Apply the Policy-Map to the Control-Plane of the
!--- device.

control-plane service-policy input drop-DLSw-traffic
```

In the above CoPP example, the access control entries (ACEs) that match the potential exploit packets with the “permit” action result in these packets being discarded by the policy-map “drop” function, while packets that match the “deny” action (not shown) are not affected by the policy-map drop function. Please note that in the Cisco IOS 12.2S and 12.0S trains, the policy-map syntax is different:

```
policy-map drop-DLSw-traffic class drop-DLSw-class police 32000 1500 1500
conform-action drop exceed-action drop
```

Additional information on the configuration and use of the CoPP feature is available at:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod_white_paper0900aecd804fa16a.html

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrtlmt.html

* Using Infrastructure ACLs at Network Boundary

Although it is often difficult to block traffic transiting your network, it is possible to identify traffic that should never be allowed to target your infrastructure devices and block that traffic at the border of your network. iACLs are a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for this specific vulnerability. The iACL example shown below should be included as part of the deployed infrastructure access-list that will protect all devices with IP addresses in the infrastructure IP address range. If FST is not used, protocol 91 may be completely filtered. Additionally, if UDP is disabled with the **dlsu udp-disable** command, UDP port 2067 may also be completely filtered.

```
!--- Permit DLSu (UDP port 2067 and IP protocol 91) packets
!--- from trusted hosts destined to infrastructure addresses.

access-list 150 permit udp TRUSTED_HOSTS MASK INFRASTRUCTURE_ADDRESSES MASK eq 2067
access-list 150 permit 91 TRUSTED_HOSTS MASK INFRASTRUCTURE_ADDRESSES MASK

!--- Deny DLSu (UDP port 2067 and IP protocol 91) packets from
!--- all other sources destined to infrastructure addresses.

access-list 150 deny udp any INFRASTRUCTURE_ADDRESSES MASK eq 2067 access-list 150
deny 91 any INFRASTRUCTURE_ADDRESSES MASK

!--- Permit/deny all other Layer 3 and Layer 4 traffic in accordance
!--- with existing security policies and configurations.
!--- Permit all other traffic to transit the device.

access-list 150 permit ip any any

interface serial 2/0 ip access-group 150 in
```

The white paper entitled “Protecting Your Core: Infrastructure Protection Access Control Lists” presents guidelines and recommended deployment techniques for infrastructure protection access lists. This white paper can be obtained at the following link:

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml

Further Problem Description: This vulnerability occurs on multiple events to be exploited. It is medium complexity in order to exploit and has never been seen in a customer environment.

- CSCsz72591

Symptoms: A router crashes with an Address Error (load or instruction fetch) exception.

Conditions: The router must be configured to act as a DHCP client.

Workaround: There is no workaround.

- CSCtd75033

Symptoms: Cisco IOS Software is affected by NTP mode 7 denial-of-service vulnerability.

Conditions: Cisco IOS Software with support for Network Time Protocol (NTP) contains a vulnerability processing specific NTP Control Mode 7 packets. This results in increased CPU on the device and increased traffic on the network segments.

This is the same as the vulnerability which is described in <http://www.kb.cert.org/vuls/id/568372>.

Cisco has release a public facing vulnerability alert at the following link:

<http://tools.cisco.com/security/center/viewAlert.x?alertId=19540>

Cisco IOS Software that has support for NTPv4 is NOT affected. NTPv4 was introduced into Cisco IOS Software: 12.4(15)XZ, 12.4(20)MR, 12.4(20)T, 12.4(20)YA, 12.4(22)GC1, 12.4(22)MD, 12.4(22)YB, 12.4(22)YD, 12.4(22)YE and 15.0(1)M.

All other versions of Cisco IOS and Cisco IOS XE Software are affected.

To see if a device is configured with NTP, log into the device and issue the CLI command **show running-config | include ntp**. If the output returns either of the following commands listed then the device is vulnerable:

```
ntp master <any following commands>
ntp peer <any following commands>
ntp server <any following commands>
ntp broadcast client
ntp multicast client
```

The following example identifies a Cisco device that is configured with NTP:

```
router#show running-config | include ntp
ntp peer 192.168.0.12
```

The following example identifies a Cisco device that is not configured with NTP:

```
router#show running-config | include ntp
router#
```

To determine the Cisco IOS Software release that is running on a Cisco product, administrators can log in to the device and issue the show version command to display the system banner. The system banner confirms that the device is running Cisco IOS Software by displaying text similar to “Cisco Internetwork Operating System Software” or “Cisco IOS Software.” The image name displays in parentheses, followed by “Version” and the Cisco IOS Software release name. Other Cisco devices do not have the show version command or may provide different output.

The following example identifies a Cisco product that is running Cisco IOS Software Release 12.3(26) with an installed image name of C2500-IS-L:

```

Router#show version
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-IS-L), Version 12.3(26), RELEASE SOFTWARE
(fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright ) 1986-2008 by cisco Systems, Inc.
Compiled Mon 17-Mar-08 14:39 by dchih

<output truncated>

```

The following example shows a product that is running Cisco IOS Software Release 12.4(20)T with an image name of C1841-ADVENTERPRISEK9-M:

```

Router#show version
Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version
12.4(20)T, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright ) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jul-08 20:25 by prod_rel_team

<output truncated>

```

Additional information about Cisco IOS Software release naming conventions is available in “White Paper: Cisco IOS Reference Guide” at the following link:

<http://www.cisco.com/warp/public/620/1.html>

Workaround: There are no workarounds other than disabling NTP on the device. The following mitigations have been identified for this vulnerability; only packets destined for any configured IP address on the device can exploit this vulnerability. Transit traffic will not exploit this vulnerability.

Note: NTP peer authentication is not a workaround and is still a vulnerable configuration.

*** NTP Access Group**

Warning: Because the feature in this vulnerability utilizes UDP as a transport, it is possible to spoof the sender’s IP address, which may defeat access control lists (ACLs) that permit communication to these ports from trusted IP addresses. Unicast Reverse Path Forwarding (Unicast RPF) should be considered to be used in conjunction to offer a better mitigation solution.

```

!--- Configure trusted peers for allowed access

access-list 1 permit 171.70.173.55

!--- Apply ACE to the NTP configuration

ntp access-group peer 1

```


For additional information on NTP access control groups, consult the document titled “Performing Basic System Management” at the following link:

http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_basic_sys_manage.html#wp1034942

* Infrastructure Access Control Lists

Warning: Because the feature in this vulnerability utilizes UDP as a transport, it is possible to spoof the sender’s IP address, which may defeat ACLs that permit communication to these ports from trusted IP addresses. Unicast RPF should be considered to be used in conjunction to offer a better mitigation solution.

Although it is often difficult to block traffic that transits a network, it is possible to identify traffic that should never be allowed to target infrastructure devices and block that traffic at the border of networks.

Infrastructure ACLs (iACLs) are a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for this specific vulnerability. The iACL example below should be included as part of the deployed infrastructure access-list, which will help protect all devices with IP addresses in the infrastructure IP address range:

```
!---
!--- Feature: Network Time Protocol (NTP)
!---

access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 123

!--- Note: If the router is acting as a NTP broadcast client
!---   via the interface command "ntp broadcast client"
!---   then broadcast and directed broadcasts must be
!---   filtered as well. The following example covers
!---   an infrastructure address space of 192.168.0.X

access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
    host 192.168.0.255 eq ntp
access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
    host 255.255.255.255 eq ntp

!--- Note: If the router is acting as a NTP multicast client
!---   via the interface command "ntp multicast client"
!---   then multicast IP packets to the mutlicast group must
!---   be filtered as well. The following example covers
!---   a NTP multicast group of 239.0.0.1 (Default is
!---   224.0.1.1)

access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
    host 239.0.0.1 eq ntp

!--- Deny NTP traffic from all other sources destined
```

```

!--- to infrastructure addresses.

access-list 150 deny udp any
      INFRASTRUCTURE_ADDRESSES WILDCARD eq 123

!--- Permit/deny all other Layer 3 and Layer 4 traffic in
!--- accordance with existing security policies and
!--- configurations. Permit all other traffic to transit the
!--- device.

access-list 150 permit ip any any

!--- Apply access-list to all interfaces (only one example
!--- shown)

interface fastEthernet 2/0
  ip access-group 150 in

```

The white paper entitled “Protecting Your Core: Infrastructure Protection Access Control Lists” presents guidelines and recommended deployment techniques for infrastructure protection access lists and is available at the following link:

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml

* Control Plane Policing

Provided under Control Plane Policing there are two examples. The first aims at preventing the injection of malicious traffic from untrusted sources, whilst the second looks at rate limiting NTP traffic to the box.

- Filtering untrusted sources to the device.

Warning: Because the feature in this vulnerability utilizes UDP as a transport, it is possible to spoof the sender's IP address, which may defeat ACLs that permit communication to these ports from trusted IP addresses. Unicast RPF should be considered to be used in conjunction to offer a better mitigation solution.

Control Plane Policing (CoPP) can be used to block untrusted UDP traffic to the device. Cisco IOS Software Releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP can be configured on a device to help protect the management and control planes and minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic that is sent to infrastructure devices in accordance with existing security policies and configurations. The CoPP example below should be included as part of the deployed CoPP, which will help protect all devices with IP addresses in the infrastructure IP address range.

```

!--- Feature: Network Time Protocol (NTP)

access-list 150 deny udp TRUSTED_SOURCE_ADDRESSES WILDCARD
      any eq 123

!--- Deny NTP traffic from all other sources destined

```

```
!--- to the device control plane.

access-list 150 permit udp any any eq 123

!--- Permit (Police or Drop)/Deny (Allow) all other Layer3 and
!--- Layer4 traffic in accordance with existing security policies
!--- and configurations for traffic that is authorized to be sent
!--- to infrastructure devices
!--- Create a Class-Map for traffic to be policed by
!--- the CoPP feature

class-map match-all drop-udp-class
  match access-group 150

!--- Create a Policy-Map that will be applied to the
!--- Control-Plane of the device.

policy-map drop-udp-traffic
  class drop-udp-class
    drop

!--- Apply the Policy-Map to the
!--- Control-Plane of the device

control-plane
  service-policy input drop-udp-traffic
```

In the above CoPP example, the access control list entries (ACEs) that match the potential exploit packets with the “permit” action result in these packets being discarded by the policy-map “drop” function, while packets that match the “deny” action (not shown) are not affected by the policy-map drop function.

- Rate Limiting the traffic to the device The CoPP example below could be included as part of the deployed CoPP, which will help protect targeted devices from processing large amounts of NTP traffic.

Warning: If the rate-limits are exceeded valid NTP traffic may also be dropped.

```
!--- Feature: Network Time Protocol (NTP)

access-list 150 permit udp any any eq 123

!--- Create a Class-Map for traffic to be policed by
!--- the CoPP feature

class-map match-all rate-udp-class
  match access-group 150
```

```

!--- Create a Policy-Map that will be applied to the
!--- Control-Plane of the device.
!--- NOTE: See section "4. Tuning the CoPP Policy" of
!--- http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html#5
!--- for more information on choosing the most
!--- appropriate traffic rates

policy-map rate-udp-traffic
class rate-udp-class
  police 10000 1500 1500 conform-action transmit
    exceed-action drop violate-action drop

!--- Apply the Policy-Map to the
!--- Control-Plane of the device

control-plane
  service-policy input drop-udp-traffic

```

Additional information on the configuration and use of the CoPP feature can be found in the documents, “Control Plane Policing Implementation Best Practices” and “Cisco IOS Software Releases 12.2 S—Control Plane Policing” at the following links:

http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html and
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrtlmt.html

- CSCsz45567

A device running Cisco IOS Software, Cisco IOS XE Software, or Cisco IOS XR Software is vulnerable to a remote denial of service condition if it is configured for Multiprotocol Label Switching (MPLS) and has support for Label Distribution Protocol (LDP).

A crafted LDP UDP packet can cause an affected device running Cisco IOS Software or Cisco IOS XE Software to reload. On devices running affected versions of Cisco IOS XR Software, such packets can cause the device to restart the mpls_ldp process.

A system is vulnerable if configured with either LDP or Tag Distribution Protocol (TDP).

Cisco has released free software updates that address this vulnerability.

Workarounds that mitigate this vulnerability are available.

This advisory is posted at:

<http://www.cisco.com/warp/public/707/cisco-sa-20100324-ldp.shtml>

Resolved Caveats—Cisco IOS Release 12.0(32)S14

Cisco IOS Release 12.0(32)S14 is a rebuild of Cisco IOS Release 12.0(32)S. The caveats listed in this section are resolved in Cisco IOS Release 12.0(32)S14 but may be open in previous Cisco IOS releases. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCse56910

Symptoms: Bundle links are added or removed when an MFR bundle is in the Administrative Down state; when the bundle is brought back to the Up state, its interface bandwidth value is not properly reflected.

Conditions: This symptom is observed with Cisco IOS Release 12.2SRB software.

Workaround: Shutting a bundle link interface down and bringing it back up can refresh the bundle interface bandwidth value.

- CSCse75697

Symptoms: When an ATM interface is configured with an IMA group and when you enter the **clock source line** command, the router may crash.

Conditions: This symptom is observed on a Cisco router that integrates the fixes for caveats CSCin90422 and CSCsb68536.

Workaround: There is no workaround.

Further Problem Description: The symptom occurs because the default clocking has been changed to “internal” via the fixes for caveats CSCin90422 and CSCsb68536. The fix for this caveat, CSCse75697, sets the default clocking back to “line.”

- CSCsf26043

Symptoms: IS-IS protocol packets may not be classified as high-priority. When this situation occurs during stress conditions and when the IS-IS protocol packets are mixed with other packets, the IS-IS protocol packets may be dropped because of their low-priority.

Conditions: This symptom is observed on a Cisco platform that is configured for Selective Packet Discard (SPD).

Workaround: Ensure that DSCP rewrite is enabled and then enter the following command:

```
mls qos protocol isis precedence 6
```

- CSCsh42820

Symptoms: Alignment correction seen on an MCT3.

Conditions: The symptom is observed when dLFiOLL is configured on a Cisco 7500 series router and an OIR is done on an MCT3 VIP.

Workaround: There is no workaround.

- CSCsh97579

Cisco devices running affected versions of Cisco IOS Software are vulnerable to a denial of service (DoS) attack if configured for IP tunnels and Cisco Express Forwarding.

Cisco has released free software updates that address this vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090923-tunnels.shtml>.

- CSCsj12565

Symptoms: Route Processor unexpectedly reloads upon removing and adding the **network x.x.x.x** command two or three times under the OSPF process.

Conditions: The symptom is observed on a GSR configured with 1500 TE tunnels in a scale setup.

Workaround: There is no workaround.

- CSCsk35688

Symptoms: Aggregate routes are not processed if all aggregated child routes are deleted prematurely.

Conditions: The symptom is observed when all aggregated child routes are marked for deletion and the periodic function which processes the routes to be deleted deletes the route before the aggregate processing function gets a chance to process them and the aggregate route to which they belong.

Workaround: Configuring “bgp aggregate-timer” to 0 or the lowest value would considerably reduce the chances of hitting this problem. In case this problem does occur, in order to delete the stale aggregate route, configure a temporary local BGP route (say, redistribute a static route or network a loopback) with its address being a subnet of the stale aggregate address and then remove the aggregate address and the added route. This should delete the route from table and send withdraws to the other routes also.

Further Problem Description: The periodic function is by default called at 60 second intervals. The aggregate processing is normally done based on the CPU load. If there is no CPU load, then the aggregate processing function would be triggered within one second. As the CPU load increases, this function call will be triggered at higher intervals and if the CPU load is very high it could go as high as the maximum aggregate timer value configured via command. By default this maximum value is 30 seconds and is configurable with a range of 6-60 seconds and in some trains 0. So, if default values are configured, then as the CPU load increases, the chances of hitting this defect is higher.

- CSCsu24425

Symptoms: Standby RP can crash upon boot up.

Conditions: The symptom is observed under the following conditions:

1. “clock timezone ..” is configured.
2. config-register = 0x2142.
3. The router is running Cisco IOS Release 12.0S based code.

Workaround: Use config-register 0x2102 and unconfigure the clock timezone.

- CSCsv27607

Symptoms: BGP router filters outbound routes to the peers when doing soft reset with specifying peer address using the **clear ip bgp ip-addr soft out** command. However, the routes to be filtered are not deleted from the routing table on the BGP peer router.

Conditions: The symptom happens when removing and then reapplying an outbound route-map. When issuing the **clear ip bgp neighbor-address soft out** command for each peer in an update-group after applying the outbound route-map filtering policy. The withdraw for filtered prefixes is sent to the first peer specified in soft reset, but the next peers in the same update-group do not withdraw the routes.

Workaround: Perform a hard BGP reset using the **clear ip bgp ip-addr** command.

- CSCsw50410

Symptoms: The following traceback is seen on the console, and all the channelized serial links on the E3 LC flap.

```
SLOT 5:1d00h: %EE48-3-INVALID_CFG_DATA: Channel 4: Invalid configuration
data. Channel type= 5
-Traceback= 40030F00 40417F44 40418208 40418444 404184B4 40418588
SLOT 5:1d00h: %EE48-3-INVALID_CFG_DATA: Channel 5: Invalid configuration
data. Channel type= 5
-Traceback= 40030F00 40417F44 40418208 40418444 404184B4 40418588
```

Conditions: This symptom occurs with all the serial links configured on a Channelized OC48-DS3/Engine 3 card. Serial interfaces flap, bringing down BGP/OSPF for no apparent reason. No configs were done.

Workaround: There is no workaround.

- CSCsx48975

Symptoms: Channelized interfaces on a Cisco 7500 series router may face txacc loss and emit interface “not transmitting” messages.

Conditions: The symptoms are observed when, for example:

1. Flapping the E1 controller; or
2. Flapping the channelized interfaces continuously.
3. Performing an OIR of the other slot.
4. Adding and removing the E1 channel groups.

Workaround:

1. Delete the channel-group and reconfigure it.
2. Use the command **test rsp stall**. This will get back the txaccs and the router will do a MEMD recarve. The expected downtime is just 2-3 seconds.

- CSCsx70889

Cisco devices running affected versions of Cisco IOS Software are vulnerable to a denial of service (DoS) attack if configured for IP tunnels and Cisco Express Forwarding.

Cisco has released free software updates that address this vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090923-tunnels.shtml>.

- CSCsx96402

Symptoms: The LC (E3/E5) crashes upon executing certain **show controller...** commands 3-4 times.

Conditions: The symptom is observed with scale configurations on MLPPP, MFR, serial interfaces with features like VRF, VPN, basic QOS, ACL, and netflow.

Workaround: There is no workaround.

- CSCsy33936

Symptoms: The CEF process is hogging the CPU because of many incomplete fibidbs, because CEF was disabled and re-enabled.

Conditions: This symptom is observed in a scale testbed when an RPR+ switchover is performed.

Workaround: There is no workaround.

- CSCsy82104

Symptoms: I/O memory leaks after several days. The output of the E1 serial interface may be blocked as well.

Conditions: The symptoms are observed on a Cisco 7200 series router that is running Cisco IOS Release 12.0(33)S and when an E1 interface serial flaps. The QoS outgoing service-policy needs to be provisioned on this serial interface.

Workaround: Remove the outgoing QoS service-policy from the flapped/blocked serial interface.

- CSCsy92142

Symptoms: The serial interface on a channelized OC48 line card stays in the UP/DOWN state after encountering Layer 1 alarms (PRID or PAIS). The interface continues to be in the UP/DOWN state even after the Layer 1 alarms are cleared.

The interface is configured for PPP encapsulation, and path level delay triggers are enabled on this interface. The link shows UP, but the PPP negotiation will be stuck in Echo Request Sent.

Conditions: This symptom is observed with a 12.0(32)S11o-based image for channelized DS3 Engine 3 line cards with alarm delay triggers configured. The problem will be seen only with momentary path level alarms.

Workaround:

1. Perform a shut/no shut on the serial interface that is in the UP/DOWN state. However, this needs manual intervention every time.
2. Remove the **alarm-delay triggers path 2500** command from the serial interface configuration. However, the side effect of this would cause the serial interface to flap.

- CSCsy96287

Symptoms: A customer experienced a single T1 flapping on controller 0/3/0. It would take between 2,500 and 3,000 path code violations and then drop and come back. It would do this about once every 15 minutes. Problems with our phones losing connectivity to a central call manager when a WAN circuit experiences a problem.

We use Multilink PPP to bundle three T1s for a 4.5-Mb circuit. If any one of the three T1s experiences even a minor issue, phones are resetting. However, we never lose Layer 3 connectivity. The edge router maintains its BGP peering across the Multilink PPP bundle, and none of our management applications ever sees a loss in connectivity.

We recently switched over to Multilink PPP from Multilink Frame due to a requirement by our MPLS provider. We did not have an issue using Multilink Frame; hence, we believe it is an issue with our configuration for Multilink PPP.

Conditions: This issue was first noticed in a 32S6r image, and some nodes running 32s11 showed similar symptoms.

Workaround: Perform a shut/no shut on the serial interface on the Cisco 12000 series side.

Further Problem Description: The root cause of this issue is that the customer was getting exposed to an inherent limitation of a timer that was being used in the T1/E1 line-state processing routine at the PLIM level. The malfunctioning of the timer would result in the PLIM not sending a line-state update message to the line card and the route processor when a link flapped, and therefore the route processor would not bring the link down even when an alarm was present on the line. This would cause blackholing of traffic for some time until the L2 times out and the protocol comes down.

- CSCsz19255

Symptoms: Tag rewrites are missing on line cards for one of the load-shareable interfaces.

Conditions: This symptom is observed on a Cisco 12000 series router that is running Cisco IOS Release 12.0(32)S11o.

Workaround: Shut/no-shut the interface.

- CSCsz55293

Symptoms: A remote third-party device is resetting the IPv6 BGP session with a Cisco 12000 router.

Conditions: BGP is exchanging only IPv6 capability with the remote EBGP peer, but IPv4 capability will be enabled by default. The remote EBGP peer is sending only IPv6 capability, and we should advertise only IPv6 prefixes because that is the capability negotiated. We are wrongly marking IPv4 capability as negotiated and advertising IPv4 prefixes, and the remote neighbor is resetting the session because IPv4 capability is not negotiated at the peer end.

Workaround: Configure a route map to deny all IPv4 prefixes, and apply it as follows:

```
Route-map deny-ipv4 deny 10
```

```
Router bgp <asnum>
address-family ipv4
Neighbor <IPv6Address> activate
Neighbor <IPv6Address> route-map <deny-ipv4> out
```

- CSCta79412

Symptoms: BGP sessions get stuck in an active state.

Conditions: The symptom is observed when using the **neighbor fall-over** command.

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.0(32)S13

Cisco IOS Release 12.0(32)S13 is a rebuild of Cisco IOS Release 12.0(32)S. The caveats listed in this section are resolved in Cisco IOS Release 12.0(32)S13 but may be open in previous Cisco IOS releases. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCsg00102

Symptoms: SSLVPN service stops accepting any new SSLVPN connections.

Conditions: A device configured for SSLVPN may stop accepting any new SSLVPN connections, due to a vulnerability in the processing of new TCP connections for SSLVPN services. If the **debug ip tcp transactions** command is enabled and this vulnerability is triggered, debug messages with connection queue limit reached will be observed.

This vulnerability is documented in two separate Cisco bug IDs, both of which are required for a full fix CSCso04657 and CSCsg00102.

- CSCsg54016

Symptoms: With ATM/MPLS with AAL5 encapsulation, the xconnect session bounces when you enter and exit PVC configuration mode without making any configuration changes.

Conditions: This symptom is observed only when the **<CmdBold>oam-ac emulation-enable</noCmdBold>** command is used.

Workaround: There is no workaround.

- CSCsl49628

Symptoms: When a VPN routing/forwarding (VRF) is deleted through the CLI, the VRF deletion never completes on the standby RP, and the VRF cannot be reconfigured at a later time.

Conditions: This symptom is observed when BGP is enabled on the router.

Workaround: There is no workaround.

- CSCsm49112

Problem Description: When eBGP sessions that carry a full routing table (200,000+ routes) are brought up, a prolonged period of 100-percent CPU utilization (5 to 7 minutes) is experienced.

During this time, the router is unresponsive in the CLI, and it stops responding to ICMP/SNMP polls.

The router is a Cisco 12406/PRP and is running Cisco IOS Release 12.0(32)S5 (c12kprp-k4p-mz.120-32.S5).

When bringing up a BGP session with a full routing table, the router seems to load the first several thousand prefixes quickly and then stops dead for several minutes before loading the rest.

Workaround: After changing the outbound prefix list on the eBGP session to a deny all (ip prefix-list test-nothing-out seq 1 deny 0.0.0.0/0 le 32), clearing the BGP session does not produce the problem anymore.

- CSCsm75818

Symptoms: Multicast data loss may be observed while changing the PIM mode of MDT-data groups in all core routers.

Conditions: The symptom is observed while changing the PIM mode of MDT-data groups from “Sparse” to “SSM” or “SSM” to “Sparse” in all core routers in a Multicast Virtual Private Network (MVPN).

Workaround: Use the **clear ip mroute MDT-data group** command.

- CSCso64050

Symptoms: Policy-map outputs are not seen in standby router. The policy is attached to the VC in the standby, but no output is seen.

Conditions: The symptom is observed when an ATM PVC is created and a service policy is attached to the PVC.

Workaround: There is no workaround.

- CSCso92169

Symptoms: A traceback is seen on the E3 and E5 line cards.

Conditions: This symptom is observed under normal traffic conditions after a **clear ip route *** command is issued.

Workaround: There is no workaround.

- CSCsq31776

Cisco devices running affected versions of Cisco IOS Software are vulnerable to a denial of service (DoS) attack if configured for IP tunnels and Cisco Express Forwarding. Cisco has released free software updates that address this vulnerability. This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090923-tunnels.shtml>.

- CSCsr61125

Symptoms: A switchover takes more time on a Cisco 7500 router.

Conditions: This symptom is observed when RPR+ is configured on the Cisco 7500.

Workaround: There is no workaround.

- CSCsu79988

Symptoms: Before this BGP aspath memory optimization, the memory consumption for aspath has increased. With this memory optimization, the memory consumption for aspath has reduced.

Workaround: There is no workaround.

- CSCsv26606

Symptoms: A 1xCHOC12 controller goes down, and all links flap.

Conditions: This symptom is observed when the **show plim datapath details** command is executed on the line card, which dumps a lot of information on the console.

Workaround: Avoid using the **show plim datapath details** command; instead, use the per-channel **show plim datapath channel-id details** command.

- CSCsv73509

Symptoms: When “no aaa new-model” is configured, authentication happens through the local even when tacacs is configured. This happens for the exec users under vty configuration.

Conditions: Configure “no aaa new-model”, configure login local under line vty 0 4 and configure login tacacs under line vty 0 4.

Workaround: There is no workaround.

- CSCsv82120

Symptoms: A CHOC12 T1 continuously flaps when the T1 link that is connected to a third-party CE router flaps. With the Cisco router, the same issue is not observed.

Conditions: This symptom is observed under the following conditions:

- Cisco IOS Release 12.0(32)S11n.
- CHOC12 T1 links with a third-party CE router.

Workaround: Disable “yellow detection” on the CHOC12 T1 link. For example, serial interface 12/0.7/6:0:

```
controller sonet 12/0
sts-1 7
no t1 6 yellow detection
! Wait for the T1 to stabilize.
t1 6 yellow detection
!
```

- CSCsw31009

Symptoms: CEF Scanner takes high CPU for sustained periods of time around 10 minutes.

Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.0(32)S11n. It is seen under the following conditions:

- When multiple eiBGP paths exist for a certain prefix and the eBGP path is recursive through the attached next-hop.
- A large number of prefixes that have one iBGP path that is recursive through an IGP route that has one path, and one iBGP path that is recursive through an IGP route that has multiple paths.
- A route modification for load-balanced prefix.

Workaround: Configure a static route.

- CSCsw47346

Symptoms: A switchover cannot be performed on a Cisco 7500 router.

Conditions: This symptom is observed when test crash is issued on a VIP console.

Workaround: There is no workaround.

- CSCsw47868

Symptoms: An IPv6 ping fails on an E3 Gigabit line card because of a PRECAM 1 Exception.

Conditions: This issue pertains to the dropping of IPv6 packets because of a precam exception on the egress side. It looked as if the profile for IPv6 was wrong when IPv4 QoS was already applied even on different subinterfaces on the same port.

Workaround:

- 1) Add/Remove an ACL.
- 2) Add/Remove the subinterface.

- CSCsw64956

Symptoms: The **no ppp lcp fast-start** command is added to all PPP-encapsulation interfaces.

Conditions: This symptom is observed after a router is upgraded from Cisco IOS Release 12.0(32)SY7 to the latest 32sy throttle image.

Workaround: There is no workaround.

- CSCsx10140

Recent research⁽¹⁾ has shown that it is possible to cause BGP sessions to remotely reset by injecting invalid data, specifically AS_CONFED_SEQUENCE data, into the AS4_PATH attribute provided to store 4-byte ASN paths. Since AS4_PATH is an optional transitive attribute, the invalid data will be transited through many intermediate ASes which will not examine the content. For this bug to be triggered, an operator does not have to be actively using 4-byte AS support.

The root cause of this problem is the Cisco implementation of RFC 4893 (4-byte ASN support) - this RFC states that AS_CONFED_SEQUENCE data in the AS4_PATH attribute is invalid. However, it does not explicitly state what to do if such invalid data is received, so the Cisco implementation of this RFC sends a BGP NOTIFICATION message to the peer and the BGP session is terminated.

RFC 4893 is in the process of getting updated to avoid this problem, and the fix for this bug implements the proposed change. The proposed change is as follows:

“To prevent the possible propagation of confederation path segments outside of a confederation, the path segment types AS_CONFED_SEQUENCE and AS_CONFED_SET [RFC5065] are declared invalid for the AS4_PATH attribute. A NEW BGP speaker MUST NOT send these path segment types in the AS4_PATH attribute of an UPDATE message. A NEW BGP speaker that receives these path segment types in the AS4_PATH attribute of an UPDATE message MUST discard these path segments, adjust the relevant attribute fields accordingly, and continue processing the UPDATE message.”

The only affected version of Cisco IOS that supports RFC 4893 is 12.0(32)S12, released in December 2008.

⁽¹⁾ For more information, please visit:

<http://www.merit.edu/mail.archives/nanog/msg14345.html>

- CSCsx32416

Symptoms: A session may go down one or more times before stabilizing in the up state.

Conditions: This symptom is observed when a BFD session is first coming up and the network is suffering from congestion.

Workaround: There is no workaround.

- CSCsx94290

Symptoms:

1) In case of a config where police rate is not taking effect on priority command, as we saw it go through default queue. This occurs in a QoS policy with a priority queue where the “police” statement occurs before the priority statement in the policy. Additionally, this occurs only upon the initial configuration of the policy-map. Editing the policy-map will correct the issue.

2) In case of a config where class is configured as only strict priority (no police) and then modified, packets go through non-default and non-priority queue.

Conditions: The initial configuration of policy-map was modified.

Workaround: Detach and re-attach the policy-map.

Resolved Caveats—Cisco IOS Release 12.0(32)S12

Cisco IOS Release 12.0(32)S12 is a rebuild of Cisco IOS Release 12.0(32)S. The caveats listed in this section are resolved in Cisco IOS Release 12.0(32)S12 but may be open in previous Cisco IOS releases. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCdw62064

Symptoms: Inbound data packets that are reassembled from multilink fragments may not be processed properly on Multilink PPP (MLP) interfaces that are receiving encrypted IP Security (IPSec) traffic that is terminated locally when a hardware accelerator is used for decryption.

Conditions: This symptom affects all inbound reassembled data frames that are received by the bundle and not just those data frames that are carrying encrypted IP datagrams. Most significantly, inbound Internet Security Association and Key Management Protocol (ISAKMP) keepalives are not processed, leading to the eventual failures of the associated IPSec sessions.

The IPSec sessions are reestablished after each failure, but traffic drops will occur until the session is renegotiated via the Internet Key Exchange (IKE). Thus, the observable symptoms are an intermittent failure of IPSec sessions combined with high loss rates in the encrypted data traffic.

Workaround: Disable hardware crypto acceleration, and use software crypto acceleration instead.

- CSCea53765

Symptoms: Adding a /31 netmask route on a Cisco router may not overwrite an existing /32 CEF entry.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.1(13)E4, Release 12.2, other 12.1E releases, or Release 12.3. Any 12.2S release past 12.2(20)S is not affected.

Workaround: There is no workaround.

Further Problem Description: The fix for this caveat enables prefixes that are derived from adjacencies in the FIB to be periodically validated against covering prefixes that originate from the RIB. Validation ensures that an adjacency prefix is only active when it points out of the same interface as a covering attached prefix. To enable this validation, enter the **ip cef table adjacency-prefix validate** global configuration command.

Note that because validation is periodic, there could be a time lag between RIB changes and subsequent validation or withdrawal of covered adjacencies in the FIB.

- CSCeg30179

Symptoms: Removing a policy that has shape and bandwidth in the same class (in that same order) may cause a router to crash.

Conditions: This symptom is observed when the router functions under a traffic load.

Workaround: There is no workaround.
- CSCei45749

Symptoms: When you enter the **clear interface** command on an Inverse Multiplexing for ATM (IMA) interface configured for dynamic bandwidth, the PVCs that are associated with the IMA interface may become Inactive.

Conditions: This symptom is observed only for IMA interfaces that have the **atm bandwidth dynamic** command enabled.

Workaround: Issuing the **no atm bandwidth dynamic** command from the IMA interface can prevent the problem from happening. If the problem has been experienced already, using the **no atm bandwidth dynamic** command followed by a **shutdown** and subsequent **no shutdown** from the IMA interface can be used to workaround the problem and clear the inactive PVC condition.
- CSCek25851

Symptoms: While adding the policer, when it gets rejected, the proper action should also detach the action from the policy map.

Conditions: This symptom is observed in the following releases:

 - 12.2(31.04.05)SR
 - 12.2(33)SXH
 - 12.2(33)SB
 - 12.0(31a)S02a

Workaround: There is no workaround.
- CSCse61893

Symptoms: A ping from a channelized T3 (CT3) port adapter may fail.

Conditions: This symptom is observed on a Cisco platform that is configured with a CT3 port adapter that functions in unchannelized mode.

Workaround: There is no workaround.
- CSCsg50187

Symptoms: CEF-switching does not function, and the output of the **show adjacency interface-type interface-number detail** command does not show any packets.

Conditions: This symptom is observed on a Cisco router when packets are switched to a multilink interface via CEF and when you enter the **show adjacency interface-type interface-number detail** command for a multilink interface.

Workaround: There is no workaround.
- CSCsh61119

Symptoms: ARP may be refreshed excessively on the default interface, causing high CPU usage in the “Collection Process.”

Conditions: This symptom is observed on a Cisco router that has point-to-point interfaces that have non-/32 interface addresses or secondary addresses and that constantly come up or go down.

Workaround: There is no workaround.

- CSCsi68795

Symptoms: A PE that is part of a confederation and that has received a VPNv4 prefix from an internal and an external confederation peer, may assign a local label to the prefix despite the fact that the prefix is not local to this PE and that the PE is not changing the BGP next-hop.

Conditions: The symptoms are observed when receiving the prefix via two paths from confederation peers.

Workaround: There is no workaround.

Further Problem Description: Whether or not the PE will chose to allocate a local label depends on the order that the multiple paths for this VPNv4 prefix are learned. The immediate impact is that the local label allocated takes up memory in the router as the router will populate the LFIB with the labels.

- CSCsi77983

Symptoms: NetFlow cache runs out of space for new flow entry when customer uses heavy traffic.

Conditions: Large amount of traffic which could exhaust the NetFlow cache.

Workaround: There is no workaround.

- CSCsi84089

Symptoms: A few seconds after OSPF adjacencies come up, a router crashes because of a bus error.

Conditions: This symptom is observed on a Cisco router that functions as an ISR that is configured for OSPF.

Workaround: Add area 0 in the OSPF VRF processes.

Alternate Workaround: Enter the **no capability transit** command in the OSPF VRF processes.

- CSCsj30417

Symptoms: In Eng3 ATM, when a subinterface flaps, traffic to certain destinations is forwarded to the wrong subinterface.

Conditions: This symptom is observed in Cisco IOS Release 12.0(32)S05 and 12.0(32)S06. The symptom is not found in Cisco IOS Release 12.0(31)S2.

Workaround: There is no workaround; however, reloading the line card solves the problem.

- CSCsj49293

Symptoms: The interface output rate (214 Mb/s) is greater than the interface line rate (155 Mb/s).

Conditions: This symptom is observed with a Cisco 7600/7500/7200-NPE400 and below. That is, PA-POS-2OC3/1OC3 (PULL mode).

Workaround: There is no workaround.

Further Problem Description: From the Ixia, packets are transmitted at 320 Mb/s. On the UUT (Cisco 7600), the outgoing interface (POS-Enhanced Flexwan) shows the output rate as 200 Mb/s. But the interface bandwidth is 155 Mb/s.

- CSCsj50773

Symptoms: Performing the **snmpwalk** on the ipRouteTable MIB may cause high CPU and reloads.

Conditions: This symptom is observed on a router that is running Cisco IOS Release 12.4(13b) or later releases.

Workaround: Create a view that excludes the ipRouteTable:

```
snmp-server view cutdown 1.3.6.1.2.1.4.21 exclude
snmp-server view cutdown internet included
snmp-server community <comm> view cutdown RO
```

This view restricts the objects that the NMS can poll. It excludes access to the ipRouteTable, but allows access to the other MIBs.

- CSCsk32095

Symptoms: The Ethernet interface flaps after configuring QoS on the interface.

Conditions: Occurs on PA-2FE-TX port adapter after applying QoS to the interface.

Workaround: There is no workaround.

- CSCsk35985

Symptoms: The system crashes when the **show ipv6 ospf lsdb-radix** hidden command is entered.

Conditions: This symptom is observed when the **show ipv6 ospf lsdb-radix** hidden command is entered.

Workaround: Do not enter the **show ipv6 ospf lsdb-radix** command.

- CSCsk64158

Symptoms: Several features within Cisco IOS software are affected by a crafted UDP packet vulnerability. If any of the affected features are enabled, a successful attack will result in a blocked input queue on the inbound interface. Only crafted UDP packets destined for the device could result in the interface being blocked, transit traffic will not block the interface.

Cisco has released free software updates that address this vulnerability.

Workarounds that mitigate this vulnerability are available in the workarounds section of the advisory. This advisory is posted at the following link:

<http://www.cisco.com/warp/public/707/cisco-sa-20090325-udp.shtml>

- CSCsk69194

Symptoms: The **shape average percent** calculation is wrong.

Conditions: This symptom is observed on a Cisco 7500 router that is configured for dLFIoLL. The policy is attached to ATM and multilink interfaces.

Workaround: Use only absolute values in the shape policy.

- CSCsk89546

Symptoms: OSPF routes are not populated in the Routing Information Base (RIB) with the next hop as traffic engineering (TE) tunnels.

Conditions: Occurs when multiple TE tunnels are configured and the tunnels come up or are shut/no shut simultaneously.

Workaround: Shut/no shut tunnels one at a time.

- CSCsl51616

Symptoms: The v6-vrf-lite configuration does not synch properly with the standby; hence 100 percent of the traffic is lost after an SSO switchover.

Conditions: The conditions under which this symptom is observed are unknown.

Workaround: There is no workaround.

- CSCsl61164

Symptoms: Router may crash @ipflow_fill_data_in_flowset when changing the flow version.

Conditions: Occurs when NetFlow is running with data export occurring while manually changing the flow-export version configuration from version 9 to version 5 and then back again to version 9.

Workaround: Do not change the NetFlow flow version while the router is exporting data and routing traffic.

- CSCsl67149

Symptoms: A sync issue is observed with the standby and active configuration.

Conditions: This symptom is observed on a Cisco 12000 series router that is configured for MLPP/MFR. When an attempt is made to remove and add the members before the unprovisioning is completed, the member is added in standby but not in active; hence the configuration sync issue.

Workaround: Add the member after the unprovisioning is completed.

- CSCsm27071

A vulnerability in the handling of IP sockets can cause devices to be vulnerable to a denial of service attack when any of several features of Cisco IOS software are enabled. A sequence of specially crafted TCP/IP packets could cause any of the following results:

- The configured feature may stop accepting new connections or sessions.
- The memory of the device may be consumed.
- The device may experience prolonged high CPU utilization.
- The device may reload. Cisco has released free software updates that address this vulnerability.

Workarounds that mitigate this vulnerability are available in the “workarounds” section of the advisory. The advisory is posted at:

<http://www.cisco.com/warp/public/707/cisco-sa-20090325-ip.shtml>

- CSCsm45113

Symptom: Router may install duplicate routes or incorrect route netmask into routing table. It could happen on any routing protocol. Additionally, for OSPF, crash was observed.

Conditions: The problem is triggered by SNMP polling of ipRouteTable MIB. The problem is introduced by CSCsj50773, see the Integrated-in field of CSCsj50773 for affected images.

Workaround: Do not poll ipRouteTable MIB, poll newer replacement ipForward MIB. instead. The ipRouteTable MIB was replaced by ipForward MIB in RFC 1354.

Further problem description: The **clear ip route *** command can correct the routing table until the next poll of ipRouteTable MIB.

- CSCsm70668

Symptoms: A soft OIR over E3:POS impacts complete traffic with a biscuit tunnel.

Condition: A soft OIR over E3:POS impacts complete traffic with a biscuit tunnel configured. In OIR “test mbus power 6 off” and “test mbus power 6 on” are performed followed by a microcode reload on slot 6.

Workaround: There is no workaround.

- CSCsm74769

Symptoms: if_num mismatch is seen in the uidb, sometimes along with the L2TPv3 bit set to zero. As a result, customer saw L2TPv3 packet drops over FR in Cisco 12000 series Internet router.

Conditions: Removing xconnect on remote PE, resulting in a session(DLCI) FLAP on the local PE. Trigger is L2TPv3 session flap; this may cause a stale CI->Uidb mapping in internal data-structures resulting in if-num mismatch in uidb if the old CI is reused by an DLCI on a different interface.

Workaround: Reload the affected line card.

- CSCso04657

Symptoms: SSLVPN service stops accepting any new SSLVPN connections.

Conditions: A device configured for SSLVPN may stop accepting any new SSLVPN connections, due to a vulnerability in the processing of new TCP connections for SSLVPN services. If “debug ip tcp transactions” is enabled and this vulnerability is triggered, debug messages with connection queue limit reached will be observed. This vulnerability is documented in two separate Cisco bug IDs, both of which are required for a full fix: CSCso04657 and CSCsg00102.

- CSCso15740

Symptoms: The “set metric” clause in the continue route-map sequence is not setting metric correctly in some particular conditions. This is also applicable in case where the nexthop setting is done via route-map with a continue clause.

Conditions: The symptom is observed on a Cisco 12000 series router that is running Cisco IOS Release 12.0(32)SY4. This is platform independent. This symptom occurs if the route-map has a continue clause and the match condition does not allow the continue clause to be executed. The following route-map sequence which has to be executed will not execute properly if the metric or nexthop of the prefix are to be modified via the route-map.

Workaround: Avoid using “continue” in a route-map and modifying metric or nexthop via the following route-map sequence.

- CSCso46427

Symptoms: A device may crash when the **show clns interface** command is issued on the wrong interface.

Conditions: The symptom is observed when there are a number (around 100 or more) CLNS interfaces on the device.

Workaround: There is no workaround.

- CSCso65266

Symptoms: A customer upgraded to Cisco IOS Release 12.0(32)Sy4, and now the customer is seeing a memory leak in the BGP process. The memory leak is happening with the BGP router process at the rcache chunk memory when the route map has a “continue” clause in the configuration.

Conditions: The leak is seen when a “continue” statement is configured in an outbound route map.

Workaround: There is no workaround.

- CSCso72996

Symptoms: A SIP601 sometimes crashes or gets an alignment error.

```
SLOT 4:Mar 17 17:59:03.877 UTC: %ALIGN-3-SPURIOUS: Spurious memory access made at
0x408C1E14 reading 0xF SLOT 4:Mar 17 17:59:03.877 UTC: %ALIGN-3- TRACE: -Traceback=
408C1E14 408C03D4 00000000 00000000 00000000 00000000 00000000 00000000
```

Conditions: The conditions under which this symptom occurs are unknown.

Workaround: There is no workaround.

- CSCso82147

Symptoms: Line card crashes when packet over SONET (POS) shared port adapter (SPA) is present.

Conditions: Occurs the first time router is reloaded.

Workaround: There is no workaround.

- CSCso82178

Symptoms: Configuring a PBR at the E5 GE subinterface may cause buffer depletion. The buffer cannot be released except by reloading the linecard.

Conditions: This symptom is observed when a PBR is configured at the subinterface.

Workaround: There is no workaround.

- CSCso84392

Symptoms: In MVPN, on the source PE, multicast packets are punted to the RP CPU, and some packets are also dropped.

Conditions: Ingress E3 and egress E5, and the TUNSEQ error message appears.

Workaround: There is no workaround.

- CSCso87348

Symptoms: A Catalyst 6500 or a Cisco 7600 may reload unexpectedly.

Conditions: Occurs when NetFlow is configured on one of the following:

- Cisco 7600 running Cisco IOS Release 12.2(33)SRC.
- Catalyst 6500 running Cisco IOS Release 12.2SXH.

Workaround: Disable NetFlow. This is done with the following commands:

no ip flow ingress
no ip flow egress
no ip route-cache flow

Enter the appropriate command for each subinterface for which NetFlow is currently configured.

Other Notes:

Only the 12.2SRC and 12.2SXH code trains are affected. The specific versions affected are 12.2(33)SXH, 12.2(33)SXH1, 12.2(33)SXH2, 12.2(33)SXH2a, 12.2(33)SRC, and 12.2(33)SRC1.

The issue is fixed in the two affected code trains from the 12.2SXH3 and 12.2SRC2 releases onwards.

The following release trains do not have this issue; 12.2(18)SXF, 12.2(33)SRA, 12.2(33)SRB, 12.2(33)SXI and all other release trains after those affected.

- CSCso88575

Symptoms: MFR bundles associated with E5 channelized based SPAs will stop forwarding traffic, an mismatch of the connection identifier (CI) of the channelized SPA is seen on CI value in the shim header of the l2 rewrite.

Conditions: This problem will occur for l2vpns only on E5 channelized based SPAs.

Workaround: Enter into interface configuration mode.

Alternate Workaround: Remove and re-add the xconnect.

- CSCso92635

Symptoms: The line card on a Cisco 10720 resets when an IP phone is connected. The “%TOASTER-2-FAULT: T1 Exception summary:” message appears.

Conditions: The line card to which the Cisco Call Manager is connected to a Cisco 10720 crashes when an IP phone is connected to the network.

Workaround: The recommended approach is to upgrade the Cisco IOS software.

- CSCsq02826

Symptoms: The MDFS state of the line card stays in a “disabled” state, which may lead to multicast traffic being punted to the RP.

Conditions: This symptom may be observed with the following sequence of operation:

1. The router is booted without configuring the **ip multicast-routing distributed** command.
2. The **ip multicast-routing distributed** command is configured.

The issue will not be seen if the **ip multicast-routing distributed** command is present in the startup configuration when the router is reloaded.

Workaround: Enter the **clear ip mds linecard slot-number** command.

- CSCsq08131

Symptoms: Ping packets of 8180 or larger cause sourcing POS linecard/SIP to reload and remain in a boot state waiting for IPC connection.

Conditions: This symptom is observed with ping packets that are sourced from PRP2 with part number 800-27058-03.

Workaround: Reload the router.

Further Problem Description: This symptom is observed only on PRP2 with part number 800-27058-03.

- CSCsq15994

Symptoms: Low CPS may be observed.

Conditions: The symptoms are seen with PPPoA and PPPoE sessions.

Workaround: There is no workaround.

- CSCsq18916

Symptoms: A copy tftp operation failed with a Socket error when the FPD of an SPA was updated or when the SPA was reloaded, OIRed.

Conditions: This symptom is related to the number of (nnets) non-virtual interfaces on the box. Depending on that, a number of SPA reloads must be done.

Workaround:

1. Reload the SPA or the router.
2. Configure one loopback interface.

- CSCsq26625

Symptoms: In a decently scaled setup, after an RPR+ switchover, the MDFS process may fail in opening IPC port.

Conditions: This symptom is observed under the following conditions:

- 15,000 total mroutes
- 5,000 global mroutes
- Approximately 110 mVRFs

Workaround: There is no workaround.

- CSCsq42001

Symptoms: The following error messages appear:

```
SLOT 5:*May 9 21:43:48.547: %LC_SPA_DMLP-1-SPAHWBUNDLEERROR: Could not perform
required operation in SPA H/w for bundle Multilink2 in bflc_cx3_dmlp_frag_on_off SLOT
5:*May 9 21:44:10.727: %SPA_CHOC_DSX-3-ERROR: Multilink2 (cmd 203) Serial5/0/1/8:0:
response parsing failed. chnl 36, bid 1 -Traceback= 40031008 408924C0 4072B1BC
40899F64 4033DB90 4033E190 4033E5C0 4033E930 4033F448 4033F600 4015B53C 4015C020 SLOT
5:*May 9 21:44:10.735: %LC_SPA_DMLP-3-CFG_FAIL: bundle Multilink2 (id 1): bay 0 err
7 (del rx link)
```

Conditions: When we remove/add/remove all members from all the configured MLP bundles once or several times, these tracebacks are seen.

Workaround: There is no workaround.

Further Problem Description: spabrg EFC mapping goes to a mismatch state, and the following is seen:

```
SLOT 5:*May 9 21:59:26.771: %SPA_CHOC_DSX-3-HDLC_CTRL_ERR: SPA 5/0: 20 TX Chnl Queue
Overflow events on HDLC Controller were encountered.
```

- CSCsq42803

Symptoms: The **hw-module slot x qos account layer2 encapsulation** command does not take effect for an AToM connection.

Conditions: This symptom is observed when xconnect is configured under a VLAN.

Workaround: There is no workaround.

- CSCsq55258

Symptoms: After a router reloads, sometimes the configuration for the gigE and POS OC12 SPA is lost from the running configuration.

Conditions: This symptom is observed when the router is reloaded.

Workaround: There is no workaround.

- CSCsq58341

Symptoms: If both L2 and L3 services co-exist on the same interface, you can no longer configure urpf on the L3 subinterface after the fix for CSCsl09772. After the router reloads, the **urpf** command will be erased from the L3 subinterface. You have to use the workaround to reapply the **urpf** command.

Conditions: This symptom is observed when both L2 and L3 services are configured on the same interface.

Workaround: Do the following:

1. Remove the L2 connection.
2. Add urpf on the L3 subinterface.
3. Re-add the L2 connection.

- CSCsq67266

Symptoms: The **pos delay triggers line** command is configurable at the interface level of E3 channelized POS interfaces.

Conditions: This symptom is observed on a Cisco 12416 Internet series router that is booted with the Cisco IOS Release 12.0(32)S nightly build of 05/19/08. The router contains an E3 CHOC48 linecard.

Workaround: There is no workaround.

- CSCsq71212

Symptoms: EFC clock interrupts are causing a line card to crash.

Conditions: The conditions under which this symptom occurs are unknown.

Workaround: There is no workaround.

- CSCsq77980

Symptoms: When traffic is flowing over the default mdt and a remote PE's edge facing slot is reloaded, slot-mask may become zero on the UUT, which also has local switching.

Conditions: This defect is observed with Cisco IOS Release 12.0(32)S11.

Workaround: Enter the **clear ip mds linecard** command for the affected slot.

- CSCsq80773

Symptoms: Slow-path multicast fragmentation is not happening correctly. One of the output interfaces is not receiving the packets in case of MVPN traffic.

Conditions: This symptom is observed with MVPN traffic with fragmentation on one of the interfaces on E5.

Workaround: There is no workaround.

- CSCsq83540

Symptoms: A Cisco 12000 works as a PE, and an Eng5 SIP line card is used to face the CE. In the VRF, the default route 0.0.0.0 is learned from the remote PE. When the problem occurs, all traffic from the CE that is forwarded via the VRF default route is dropped.

Conditions: This symptom is observed on a Cisco 12000 Eng5 SIP line card that is running Cisco IOS Release 12.0(32)SY04, 12.0(32)SY05, or 12.0(32)SY06. When VRFs are created and deleted, new VRFs that are created will have a problem if they are allocated with a table ID allocated for older deleted VRFs.

Workaround:

1. Reload the ingress Eng5 line card that is facing the CE.

or

2. If the customer does not want to reload the line card, a second workaround can be attempted, but it is not a reliable workaround and may not always be successful. Create a new VRF without removing any VRFs, which gets a new table ID, and apply the VRF configuration completely wherever the old VRF configuration is applied.

Further Problem Description: This problem cannot be cleared by using the **clear cef linecard x** or **clear ip route vrf xxx 0.0.0.0** commands.

- CSCsq93004

Symptoms: Removal of a subinterface may cause memory corruption or a crash. The symptoms are unpredictable.

Conditions: The symptoms are rare and will be observed only if a subinterface is configured for **mpls traffic-eng auto-tunnel primary use**, and the subinterface is later removed from the configuration.

Workaround: Do not remove subinterfaces.

- CSCsr11332

Symptoms: In rare situations, the **show controller SONET port** command might crash the RP.

Conditions: This symptom has been observed on a 4CHOC12/DS3-I-SCB= line card, but it can be seen on other similar channelized line cards. It may be reproducible by executing the **show controller SONET port** command on a nonexistent port like sonet 3/4 (that is, only sonet 0/0, 0/1, 0/2, and 0/3 are valid on a 4CHOC line card). When the problem can be seen, the CLI help indicates an incorrect unit number:

```
Router# show controller sonet 12/?  
<0-48> Controller unit number
```

If the controller unit number is shown fine (for example, <0-3>), then the crash will not occur.

Workaround: There is no workaround.

- CSCsr13314

Symptoms: The **pos delay triggers line** command is configurable on APS-enabled interfaces of E3 clear channel POS line cards. After the commit of CSCsq45452, the **pos delay triggers path** command is not configurable on APS-enabled interfaces of E3 channelized POS line cards.

Conditions: This symptom is observed on a Cisco 12000 series Internet router that is booted with Cisco IOS Release 12.0(32)S. The router contains ISE OC48 POS and ISE CHOC48 POS line cards.

Workaround: There is no workaround.

- CSCsr20377

Due to an eng3 hardware limitation, there is more overhead added to like to like Ethernet PW or Ethernet interworking PW if “hw-module slot <> qos account layer2 encapsulation length <>” is configured. Without the fix of CSCsq42803, the overhead impact is less. Request a return to the behavior of 12.0(32)SY back to pre-CSCsq42803.

- CSCsr22043

Symptoms: A controller goes into an admin down state.

Conditions: This symptom is observed when an STS path under the SONET controller is shut down.

Workaround: Perform a no shutdown on the controller.

- CSCsr42364

Symptoms: All line cards may crash after a switchover in Route Processor Redundancy Plus mode.

Conditions: This issue is observed on Cisco 12000 series Internet routers with PRP2 processors. This issue usually requires multiple line-card reloads prior to the switchover. It is seen under conditions of high line-card utilization.

Workaround: There is no workaround.

- CSCsr47477

Symptoms: After a router reloads, sometimes there may be mbus message gets timed out on the SIP601 located in the lower cage of a Cisco 12816.

Conditions: This symptom is observed after a router reloads.

Workaround: There is no workaround.

- CSCsr47795

Symptoms: After flapping the interfaces, the FIB converges and points to the correct outgoing interface, while the FIB in hardware points to another interface.

The trigger is when the interface is flapping because the default route is updated. The BGP session is always stable and never goes down.

Topology:

End customer -----(eng3)slot4 c12k_Lab_router-42 slot5 and slot6(Eng5) ----- router_B -----
Internet

The Lab-router-42 router receives a default route from the router_B neighbor.

Snapshots from the Eng3 line card on slot4:

Lab-router-42# exec slot 4 show ip hardware-cef 10.1.1.1 detail

===== Line Card (Slot 4) =====

Root: 0x240CE000 Location: 0x240CE404 Data: 0x81819380 Offset: 0x93D96404 Leaf pointer:
0x300C9C00

Leaf FCR 2 Addr 0x300C9C00 : 0xE0000100 0x0285C008 found 2 deep SRAM Loadbalance addr
0x28170020 default alpha ip loadbalance: 0x28170020 (0 paths, hw maxpath 0) Hash 1: alpha
adjacency: 0x2001FA60 (cef adj NULL or alpha_default_lb) [0] oi 0x200006 oq 4080 in A ab 50 hl
20 gp 19 tl 4 loq 9800 6/0/0 mtu 1520 Output interface is GigabitEthernet6/0/0 <== Here ^^^^^
Here

1 tag: 23 current counters 95059, 5157246 last reported 93252, 5059668

Output Queue / Local Output Queue Bundle: [0-7] output queue 0x4080 local output queue 0x9800
PLU leaf data: 0xE0000100 0x0285C008 0xA1020304 0xA5080000 Mask bits: 1 Origin AS: 0
Source lookup drop: yes QOS group: 0 Traffic index: 0 Precedence not set Default Route: yes PBR
enabled: no

While the FIB was updated to the proper outgoing interface.

LAB_router_42# exec slot 4 show ip cef 10.1.1.1

===== Line Card (Slot 4) =====

0.0.0.0/0, version 38, epoch 0, cached adjacency 10.125.72.74 0 packets, 0 bytes Flow: AS 0, mask
0 tag information from 10.38.192.6/32, shared, all rewrites owned local tag: 34 via 192.168.225.0,
0 dependencies, recursive next hop 10.125.72.74, GigabitEthernet5/0/0 via 192.168.225.0/24
(Default) <=== HERE valid cached adjacency tag rewrite with Gi5/0/0, 10.125.72.74, tags imposed
{ } <=== HERE LAB_router_42#

Conditions: This symptom is observed when there is a default route configured while running
Cisco IOS Release 120(32)SY4 or 120(32)SY6 on Eng3.

Workaround: Clear ip route 0.0.0.0 or <default-network>.

- CSCsr64777

Symptoms: A router crashes because of a block overrun (overwriting the memory block).

Conditions: This symptom is observed only when NetFlow version 5 is used.

Workaround: NetFlow version 9 could be used for exporting.

- CSCsr67137

Symptoms: An Engine 3 (E3) Channelized OC12 (CHOC12) line card can reload after a switchover
in Route Processor Redundancy Plus (RPR+) mode.

Conditions: This symptom is observed on a Cisco 12416 Internet series router. The router is booted
with Cisco IOS Release 12.0(32)S11n and contains the following:

- Redundant PRP-2 processor running in RPR+ mode
- E3 CHOC12 line card
- All other slots in the chassis are populated with E3, E4+, and E5 line cards.

Workaround: There is no workaround.

- CSCsr67289
Symptoms: Router hangs when online insertion and removal (OIR) is performed.
Conditions: Occurs after changing the interface bandwidth followed by an OIR operation.
Workaround: Stop traffic before making these changes.
- CSCsr70530
Symptoms: A line card crashes.
Conditions: This symptom is observed after members of the MLPPP are swapped from one bay to another bay and vice-versa on the same line card.
Workaround: There is no workaround.
- CSCsr70985
Symptoms: A Cisco router crashes following multiple accesses to NVRAM.
Conditions: This symptom has been observed on a Cisco 12000 series Internet router that is running Cisco IOS Release 12.0(32)SY5 when the “dir tar:” command is executed parallel with the “write memory” command. It may not be platform specific.
Workaround: Avoid using the “dir tar:” command.
- CSCsr79573
Symptoms: The member link of a multilink bundle goes into an up/down state.
Conditions: This symptom is observed when multilink is swapped from one multilink bundle to another multilink bundle through a script.
Workaround: Enter the “hw-module subslot <slot#/subslot#> reload” command.
- CSCsr80321
Symptoms: Commands cannot be sent to the SPA.
Conditions: This symptom is observed when the members of MLPPP and MLFR are swapped.
Workaround: Reload the line card.
- CSCsr83626
Symptoms: The line card in slot 0 does not boot up completely. It does not go past the UP IOS state.
Conditions: This symptom is observed after upgrading the router to Cisco IOS Release 12.0(32)SY5 and having the ATM line card in slot 6 send an LAIS alarm.
Workaround: Move the ATM card to another slot, or shut down the ATM line card in slot 6.
- CSCsu09595
Symptoms: A SIP-601 crashes while changing the CRC/encap/MTU on MLPPP and MFR.
Conditions: This symptom is observed under the following conditions:
 1. Change the CRC of the members of the bundle (from crc 16 to 32 and then back again to crc 16).
 2. Remove the members from the bundle.
 3. Add serials back to MFR and MLPPP.
 4. Change the MTU.
 5. Flap the links (serials and bundle).
Workaround: There is no workaround.
- CSCsu12146
Symptoms: On a Cisco 12404 that is running Cisco IOS Release 12.0(32)SY5, a SIP-401 reloads when lawful intercept (LI) is used on it.
Conditions: This symptom is observed when LI is activated.

Workaround: Deactivate LI.

- CSCsu21668

Symptoms: “carve-level 0” is being used in SY5 nodes (SIP-601) to avoid unnecessary buffer recarving and subsequent traffic disruption.

Conditions:

carve-level 0

Workaround: There is no workaround.

- CSCsu32015

Symptoms: A ping fails across Frame Relay subinterfaces over a non- channelized SPA.

Conditions: The ping fails across Frame Relay subinterfaces when:

- The channelized SPA is used on a bay and there are approximately 30 or more interfaces that are created and used.
- That SPA is later removed and moved to some other bay or to some other slot.
- And this current empty bay is then used for a non-channelized SPA and for Frame Relay subinterface circuits.

Workaround: There is no workaround.

- CSCsu33246

Symptoms: IPv6 PIM RP embedded functionality is not working properly in Cisco IOS Release 12.0(32)S or Release 12.0(32)SY even after the fix for CSCsf28907.

Conditions: If a first-hop router (that is connected to the IPv6 multicast source) is configured for a PIM RP embedded operation, the register packets will not be sent to the RP and the mroute table will remain in the Registering state. No IPv6 multicast traffic will flow.

Workaround: Configure an IPv6 PIM static RP.

- CSCsu41968

Symptoms: On a Cisco 7500 with an HA setup, the “show controller t3” command is showing framing as M23 on the active and as C-bit on the standby. So the “loopback remote” configuration is rejected on the active and is accepted on the standby.

Conditions: This symptom is observed when the “show controller t3 1/1/0” command is issued.

Workaround: There is no workaround.

Further Problem Description: Because of the framing mismatch, the standby might crash due to sync issues.

- CSCsu63081

Symptoms: The **delay triggers path** *delay* command does not function as it is provisioned on an E3 CHOC12 controller.

Conditions: This symptom is observed on a Cisco 12000 Internet series router booted with c12kprp-p-mz.120-32.S11n. This router contains an E3 CHOC12 line card.

Workaround: There is no workaround.

- CSCsu86288

Symptoms: A line card on a Cisco 12000 series Internet router generates tracebacks during LI provisioning while installing a 50th tap request. After the appearance of the first traceback, LI functionality stops working for newly requested taps.

Conditions: This symptom is observed when there are 48 active taps and 2 new taps arrive.

Workaround: Reload the line card or the whole router.

- CSCsu92317

Symptoms: Pings fail on an MLPPP interface.

Conditions: There is an MFR interface used for L2 services such as xconnect and an MLPPP interface on the same SPA. When the member links are removed/added from these bundles back-to-back, the ping on the MLPPP interface may fail. This symptom is observed so far only on E5 cards.

Workaround: Reload the line card.

- CSCsv04836

Multiple Cisco products are affected by denial of service (DoS) vulnerabilities that manipulate the state of Transmission Control Protocol (TCP) connections. By manipulating the state of a TCP connection, an attacker could force the TCP connection to remain in a long-lived state, possibly indefinitely. If enough TCP connections are forced into a long-lived or indefinite state, resources on a system under attack may be consumed, preventing new TCP connections from being accepted. In some cases, a system reboot may be necessary to recover normal system operation. To exploit these vulnerabilities, an attacker must be able to complete a TCP three-way handshake with a vulnerable system.

In addition to these vulnerabilities, Cisco Nexus 5000 devices contain a TCP DoS vulnerability that may result in a system crash. This additional vulnerability was found as a result of testing the TCP state manipulation vulnerabilities.

Cisco has released free software updates for download from the Cisco website that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090908-tcp24.shtml>.

- CSCsv08408

Symptoms: A router may crash due to a bus error due to an illegal access to a low address because IPC is processing a message that is already returned back to the pool, but still the message's reference is present in IPC's retry table.

Conditions: The conditions under which this symptom occurs are not known.

Workaround: There is no workaround.

- CSCsv27470

Symptoms: An Engine 3 CHOC12 fails to bring the T1 controller link down when the **delay triggers path** command is configured.

Conditions: Shutting down the remote end T1 controller or CHOC12 T1 controller receive AIS will not cause the T1 link to go to down state.

Workaround: Do not configure the **delay triggers path** command on the CHOC12 SONET controller.

- CSCsv38557

Symptoms: POS interfaces run into a tx stuck condition, and heavy packet drops occur in the local switching path. The VIP CPU runs high due to the Rx-Side Buffering mechanism that kick starts in the local switching path in the VIP.

Conditions: This symptom is observed on a Cisco 7500 node with a VIP that has the POS interfaces up and data traffic being locally switched between the POS interfaces. This symptoms is triggered when a service policy is applied/removed followed by interface flaps.

Workaround: “test rsp stall” cleans up the Rx-Side buffered packets. Hence this could be considered a workaround. However, this does not always help. Doing a soft OIR removal and insertion of the LC always helps recover from this situation. The best workaround is to apply a service policy.

- CSCuk61422

Symptoms: CEF-switching does not function, and the output of the **show adjacency interface-type interface-number detail** command does not show any packets.

Conditions: This symptom is observed on a Cisco 7500 series that has an RSP when packets are switched to a multilink interface via CEF and when you enter the **show adjacency interface-type interface-number detail** command for a multilink interface.

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.0(32)S11

Cisco IOS Release 12.0(32)S11 is a rebuild of Cisco IOS Release 12.0(32)S. The caveats listed in this section are resolved in Cisco IOS Release 12.0(32)S11 but may be open in previous Cisco IOS releases. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCee73956

Symptoms: The Generalized TTL Security Mechanism (GTSM), formerly known as BGP TTL Security Hack (BTSH), checks the time-to-live (TTL) value of the packets at the application level, which is not efficient. Also, GTSM does not stop the establishment of a TCP connection for a packet with an invalid TTL value.

Conditions: This symptom is observed on a Cisco platform that has the **neighbor neighbor-address security ttl hops hop-count** command configured in a BGP environment.

Workaround: There is no workaround.

- CSCef70161

Symptoms: External BGP neighbors that are configured in the IPv4 VRF address-family context may fall into different update groups, even if the outbound policy is identical. This situation slightly reduces the overall scalability because BGP cannot use update replication when sending updates to the neighbors.

Conditions: This symptom is observed on a Cisco router and is both release- and platform-independent.

Workaround: There is no workaround.

Further Problem Description: The symptom does not affect neighbors that are configured in the global IPv4 address-family context.

- CSCeg25475

Symptoms: Filtering BGP routes by means of the **distribute-list prefix MARTIAN in** command applied to address-family IPv4 actually filters out M-BGP routes in address-family VPNv4.

Conditions: This symptom occurs when MPLS-VPNs are configured.

Workaround: Use route maps to filter routes inbound.

Further Problem Description: The **show ip bgp neighbors** command can be used to check whether the prefixes are actually being filtered out from updates for address-family VPNv4, and not for IPv4, as it is configured.

- CSCsa73179

Symptoms: Memory corruption, possibly leading to a crash or other undesired behavior, can occur when the **no default-information originate** command is entered in router RIP configuration mode.

Conditions: This symptom occurs only if both the RIP routing protocol and the OSPF routing protocol are configured on a router.

Workaround: There is no workaround.

- CSCsd46413

Symptoms: Long configuration times are seen for very large QoS configurations (at or near 40,000 unique policy-map instances) for ATM PVC with policy-map per PVC.

Conditions: This symptom has been observed with very large QoS configurations and Cisco IOS Release 12.0S, Release 12.2SB, or Release 12.4T.

Workaround: There is no workaround.

- CSCsd87844

Symptoms: When a route distinguisher (RD) that is configured for a VRF is deleted and then reconfigured, the standby RP may reload unexpectedly.

Conditions: This symptom is observed on a Cisco router that has dual RPs that function in HA mode and that is configured for MPLS VPN.

Workaround: Delete the VRF itself and then reconfigure the VRF in order to change the RD. If this is not an option, there is no workaround.

Further Problem Description: The symptom occurs because the processing of the **no rd** command is completed only on the active RP. On the standby RP, the processing does not clear a flag that signals the completion of the processing of the **no rd** command. Then, when the RD is reconfigured, the configuration succeeds on the active RP but fails on the standby RP, causing the standby RP to reload.

- CSCse05292

Symptoms: A static map configuration for an ATM PVC that uses the **protocol ip ip-address** command is rejected, giving an ambiguous command error.

Conditions: This symptom is observed when you configure a static map on an ATM PVC using the **protocol ip ip-address** command.

Workaround: Explicitly configure the [**broadcast | no broadcast**] option:

```
Router(config-if-atm-vc)# protocol ip 10.10.100.2 broadcast
```

```
Router(config-if-atm-vc)# protocol ip 10.10.100.2 ?
```

```
<cr>
```

```
broadcast Pseudo-broadcast
```

```
no Prevent Pseudo-broadcast on this connection
```

```
<cr>
```

```
Router(config-if-atm-vc)# protocol ip 10.10.100.2 no broadcast
```

```
Router(config-if-atm-vc)#
```

- CSCse27461

Symptoms: If a Cisco 12000 series Internet router is configured as a PE VPN router in a large scale configuration, sometimes one or more line cards can reload during RPR+ switchback from default standby PRP (now in active role) to default primary PRP (now in standby role). Between the silent reloads or resets tracked separately, some mbus-related crashes were captured.

Conditions: This symptom has been observed in Cisco IOS Release 12.0(32)S2, on routers with scaled configurations, after RPR+ switchovers.

Workaround: There is no workaround.

- CSCse50781

Symptoms: After executing the **no ipv6 multicast-routing** command on a dual-RP router, IPC communication to the standby RP may be broken, and the following messages may be seen every minute:

```
%IPCGRP-3-ERROR: standby set time: timeout seen
```

Conditions: This symptom is observed on a Cisco 12000 series router that is running the c12kprp-p-mz image of Cisco IOS Release 12.0(32)SY.

Workaround: Reload the router.

Further Problem Description: This bug is seen only while operating in SSO mode (not in RPR mode).

- CSCse52184

Symptoms: Traffic may be interrupted for a short duration because of FIB updates. This issue happens very frequently and affects traffic forwarding.

Conditions: This issue is seen when MPLS TE tunnels are configured.

This issue is triggered when an interface is shut down and then brought back up if that interface is carrying a large rate of traffic. The problem is intensified by two factors:

1) Tunnel interface is kept flapping because of:

- a) Reoptimization
- b) Connection down

2) One tunnel flapping could trigger entire (or a very large number of) FIB updates.

So if we do not have 2), then traffic may just be lost for a very short duration, and it will not impact application.

Workaround: There is no workaround.

- CSCse56501

A device running Cisco IOS software that has Internet Protocol version 6 (IPv6) enabled may be subject to a denial of service (DoS) attack. For the device to be affected by this vulnerability the device also has to have certain Internet Protocol version 4 (IPv4) User Datagram Protocol (UDP) services enabled. To exploit this vulnerability an offending IPv6 packet must be targeted to the device. Packets that are routed throughout the router can not trigger this vulnerability. Successful exploitation will prevent the interface from receiving any additional traffic. The only exception is Resource Reservation Protocol (RSVP) service, which if exploited, will cause the device to crash. Only the interface on which the vulnerability was exploited will be affected.

Cisco is providing fixed software to address this issue. There are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at:

<http://www.cisco.com/warp/public/707/cisco-sa-20080326-IPv4IPv6.shtml>

- CSCsf20947

Symptoms: A default route that is originated and advertised to a BGP peer using the **neighbor default-originate** command may be ignored by the peer in favor of a traditional default route (from the BGP table) that is advertised to the same peer.

Conditions: This symptom is observed on a Cisco router after a route flap in the network causes the traditional 0.0.0.0/0 default route to be relearned by a router. In turn, the router advertises this default route to its peers, overriding the previously sent default-originate route. The result is that the BGP peer router learns the default route that has been propagated through the network, rather than the default route that has been created using the **neighbor default-originate** command on the adjacent router.

Workaround: Manually clear the BGP neighbor to enable the peer router to correctly relearn the correct default route (the one generated by the **neighbor default-originate** command).

- CSCsf28907

Symptoms: Embedded RP does not work in Cisco IOS Release 12.0(32)S or later releases.

Conditions: This symptom is observed on Cisco 12000 and Cisco 10720 routers with IPv6 multicast routing in Cisco IOS Release 12.0(32)S or later releases.

Workaround: Enter the **no ipv6 pim rp embedded** command and then the **ipv6 pim rp embedded** command in the global configuration mode.

- CSCsf29803

Symptoms: An engine 3 linecard in an mVPN PE router with multicast egress QoS configured may report the following error message and may also reload after this message:

```
SLOT 10:Sep 5 15:12:43.879 UTC: %EE48-3-CONGA_MCAST: Table indices not linked:
(tbl1=262129, tbl2=262136, prev=0, oiq_id=0, oi=0, oq=0)
```

Conditions: This symptom is observed when an engine 3 linecard in an mVPN PE router has both core interfaces and VRF interfaces configured and an output service policy applied to one or more of these interfaces.

Workaround: Limit engine 3 linecards with service policies to either core interfaces or VRF interfaces, and do not combine both interface types on a single linecard. Note that Cisco recommends that core and VRF interfaces not be configured on the same linecard anyway because any multicast packet that needs to egress on both interfaces will be software-forwarded and not hardware-forwarded. Alternatively, replace the engine 3 linecard with an engine 5 linecard.

- CSCsg25995

Symptoms: Networks do not show up in the BGP table for multicast address family, as can be seen in the output of the **show ip mbgp** command.

Conditions: This symptom is observed when BGP is used for multicast address family; it does not affect unicast address family.

Workaround: Use the **clear ip bgp neighbor-address** command.

- CSCsg32689

Symptoms: A crash or traceback may occur when the route-map option for fall-over is configured for a BGP peer-session template or peer group.

Conditions: This symptom occurs when the **fall-over [route-map map-name]** command is configured under the **router bgp autonomous-system-number** command.

Workaround: There is no workaround. Avoid using the route-map option.

- CSCsg35077

Symptoms: A device that is running Cisco IOS software may crash during processing of an Internet Key Exchange (IKE) message.

Conditions: The device must have a valid and complete configuration for IPsec. IPsec VPN features in Cisco IOS software that use IKE include Site-to-Site VPN tunnels, EzVPN (server and remote), DMVPN, IPsec over GRE, and GET VPN.

Workaround: Customers that do not require IPsec functionality on their devices can use the **no crypto isakmp enable** command in global configuration mode to disable the processing of IKE messages and eliminate device exposure.

If IPsec is configured, this bug may be mitigated by applying access control lists that limit the hosts or IP networks that are allowed to establish IPsec sessions with affected devices. This assumes that IPsec peers are known. This workaround may not be feasible for remote access VPN gateways where the source IP addresses of VPN clients are not known in advance. ISAKMP uses port UDP/500 and can also use UDP/848 (the GDOI port) when GDOI is in use.

Further Problem Description: This bug is triggered deep into the IKE negotiation, and an exchange of messages between IKE peers is necessary.

If IPsec is not configured, it is not possible to reach the point in the IKE negotiation where the bug exists.

- CSCsg52336

Symptoms: A router may crash when you remove an unused and unassigned VRF by entering the **no ip vrf vpn-name** command.

Conditions: This symptom is observed on a Cisco router that functions as a PE router and that has the Multi-VRF capability for OSPF routing configured along with other VRFs that are unused and unassigned.

Workaround: There is no workaround.

- CSCsg89512

Symptoms: In an MVPN topology, sparse mode, Auto RP, if the PE router has the same line card as the core and customer-facing router, and if there are two RP announcers, the RP point may not be selected correctly, and traffic will not go through.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(33)S.

Workaround: Select values for offset using the **hw-module slot x ip multicast hw-accelerate source-table size a offset b** command, which will prevent collision from happening.

- CSCsh43283

Symptoms: Engine 2 line cards stop forwarding multicast traffic when the **hw-module slot 2 ip multicast hw-accelerate** command is issued.

Conditions: This symptom is observed when a higher priority bundle such as uRPF is already running.

Workaround: Unconfigure all the features to revert back to the vanilla bundle, and then reconfigure only the features that do not collide.

- CSCsj22472

Symptoms: When an IXIA-simulated BGP neighbor is not up, BGP is forced to delete the ARP entry for the IXIA host for a while. During that period, the router has to send ARP, and traffic is lost for a while.

Conditions: While observed with other protocols, this symptom was noticed with a typical BGP configuration in which the peers are nonexistent. This would cause the SYN to be retransmitted multiple times, and after some threshold, the ARP entry would be purged.

The ARP entries gets flushed out when the TCP retransmission timer expires. This causes the CEF adjacency to be lost, and performance can drop for packets going to that destination until the ARP is resolved again. This problem is *not* specific to BGP and is applicable to anything that rides over TCP.

Workaround: There is no workaround.

- CSCsj28800

Symptoms: The Engine 5 line cards on a router crash.

Conditions: When a router is configured to have TE tunnels with CBTS, and when the **clear cef linecard** command is executed, the Engine 5 line cards on the router crash. This problem is seen in any of the Cisco IOS Release 12.0(32)SY releases prior to Cisco IOS Release 12.0(32)SY5.

Workaround: There is no workaround.

- CSCsj31964

Symptoms: The BFD protocol may go down if an interface is congested.

Conditions: This symptom is observed on a SIP-401 when 2-Gbps traffic is directed toward a Gigabit Ethernet interface that has a BFD session.

Workaround: On an Engine5 line card, apply 1CnD, nCnD service policy to map precedence 6 packets to low-latency queue. On an Engine3 line card, there is no workaround.

Further Problem Description: The problem is seen on both Engine3 and Engine5 line cards.

- CSCsj68299

Symptoms: The line card crashes when the interface MTU is changed.

Conditions: This symptom is observed when having both ingress and egress E0 cards with MPLS in the core and when an ATOM tunnel is configured on the egress line card.

Workaround: Before changing the MTU, stop the traffic across all the E0 line card interfaces. You can resume traffic after changing the MTU.

- CSCsj74173

Symptoms: Egress E0 - Two ports OC3 channelized to DS1/E1 are crashing continuously just as traffic starts.

Conditions: E0 - In an IP->Tag fragmentation case with E4/E4P/E6 POS cards as the ingress and E0 as the egress card, for certain frame sizes larger than the egress MTU, the E0 egress card crashes. This happens only with the E0 card as egress.

Workaround: Make sure that the packets sent are less than the egress MTU of the E0 linecard to avoid any fragmentation.

- CSCsj99269

Symptoms: With some VPN configurations, such as configurations with a multipath import or an import map, the CPU usage of the router may be very high for a long time, even after BGP convergence has occurred.

Conditions: This symptom is observed on a Cisco router that functions in a highly scaled environment involving several hundred VRFs and occurs after the router has been reloaded or after a switchover has occurred.

Workaround: There is no workaround.

- CSCsk55768

Symptoms: IP connectivity is lost upon the occurrence of a short flap (microflap) in the optical signal.

Conditions: No particular conditions trigger this situation.

Workaround: There is no workaround.

- CSCsk98123

Symptoms: Tx traffic may get dropped due to a “precam 1 exception.”

Conditions: This symptom is observed when vrf vlite and strict urpf are configured on the interfaces. This happens in all releases when adjacency indexes between 65528 to 65531 are used in TX SRAM Adjacency programming on line cards. This happens only on port 0. Strict URPF not a required condition. It can happen without that.

Workaround: To recover from the situation, remove and re-apply the configuration on the interface when the problem is seen. To recover from the condition, shut and no shut of the interface is fine provided it does not get adjacency index allocated within 65528 and 65532. If URPF/PBR is configured or removed, then also it gets cleared.

Alternate Workaround: Do not use port 0 on the line card. Using a subinterface will mitigate the issue.

- CSCsl05174

Symptoms:

- Issue 1: A non-deleted PPP configuration inside the interface reappears when the interface is created again.
- Issue 2: Some multilink configuration is not being synced to the standby (hold-queue).

Conditions: This symptom is observed when running RPR+.

Workaround: Reapply the original configuration.

Further Problem Description: Deletion of a multilink interface and subsequent creation using the same name may cause portions of the original configuration to return even if not explicitly configured. The **hold-queue** command is not being synchronized to the standby RP.

- CSCsl36013

Symptoms: A Cisco 12000 series router with an Engine 0 ATM OC12 line card may experience a problem in which a Layer 2 adjacency rewrite string for an ATM PVC becomes invalid. The invalid rewrite results in packets being forwarded out the interface with the wrong Layer 2 details prepended.

Conditions: This symptoms is observed on a Cisco 12000 series router with an Engine 0 ATM OC12 line card.

Workaround: Use the following command for the affected IP address:

clear ip arp x.x.x.x

Further Problem Description: This problem can be identified using the **execute-on [slot#] show controller rewrite** Cisco IOS command, compared to the rewrite string in the **show adjacency internal** command:

Router# **execute-on 1 show controller rewrite**

===== Line Card (Slot 1) =====

LocalMAC rewrite table

Interface	Address	Output_Info

...		
ATM1/0.1	192.168.1.1	0x1C062340
	4BA72000AABA031180C2000700000004	
	757122D600081008B0560800 <-- incorrect	
...		

Router# **execute-on all show adjacency internal**

===== Line Card (Slot 1) =====

Protocol	Interface	Address
...		
IP	ATM1/0.1	192.168.1.1(9)
131229862 packets, 74135640171 bytes		
02710100AABA031180C2000700000017		
E0DC040200072009B0450800 <-- correct		
...		

Router# **clear ip arp 192.168.1.1**

Router# **execute-on 1 show controller rewrite**

===== Line Card (Slot 1) =====

Local MAC rewrite table

Interface	Address	Output_Info
...		
ATM1/0.1	192.168.1.1	0x1C025340
6EA82000AABA031180C2000700000017		
E0DC040200072009B0450800 <-- correct		
...		

- CSCsl36723

Symptoms: A SIP401/SIP600 may crash upon a primary CSC failover. FIA Halt related error messages are also seen.

Conditions: This symptom is observed upon a primary CSC failover.

Workaround: There is no workaround.

- CSCsl43782

Symptoms: A CE-CE ping is failing in ATM-Ethernet/VLAN/ATM, PW/LS routed interworking scenarios.

Condition: This symptom is observed when the E3 ATM is in the CE side.

Workaround: There is no workaround.

- CSCsl68227

Symptoms: An E3 linecard may drop packets larger than a certain size because of a buffer carving problem when the mtu command is used for multilink interfaces.

Conditions: This symptom is observed with images based on Cisco IOS Release 12.0(32)S10.

Workaround: Changing the MTU or reloading the linecard may clear the problem.

- CSCsl89425

Symptoms: Bidirectional Forwarding Detection (BFD) sessions do not scale. This symptom is especially visible with an OSPF client when one of the peers is rebooted after configuring the maximum number of BFD sessions.

Conditions: This symptom occurs when configuring maximum BFD sessions or total number of BFD sessions too close to the maximum limit.

Workaround: Configure 90 percent of the maximum allowed BFD sessions.

- CSCsI93596
Symptoms: When the MTU is changed on the core-facing E0 LC, all the E0 cards in the router crash.
Conditions: This symptom is observed with bidirectional traffic with an L3VPN, L2VPN configuration. There are also MPLS TE tunnels.
Workaround: There is no workaround.
- CSCsI96577
Symptoms: The **show ppp multilink** statistics are not updated on a Cisco 7500 router.
Conditions: This symptom is observed when dLFioLL+SSO is configured on the Cisco 7500 router and a switchover is performed.
Workaround: There is no workaround.
- CSCsm07692
Symptoms: A SIP600 crashes.
Conditions: When the primary CSC is shut, the SIP600 crashes.
Workaround: There is no workaround.
- CSCsm10560
Symptoms: A standby route processor crashes with a traceback when multilink is provisioned/unprovisioned continuously.
Conditions: This symptom is observed with a script. There is a small but significant chance of encountering this symptom during manual testing. This symptom occurs in branches based on Cisco IOS Release 12.0S *only*.
Workaround: There is no workaround.
- CSCsm26130
Symptoms: When removing a subinterface from the configuration that contains an IP address that falls into the major net of the static route, the static route is no longer injected into the BGP table. Since the route is not in the BGP table, it is not advertised to any peers.
Conditions: This symptom is observed with auto-summary enabled in BGP. A static summary route is configured to null0 and is injected into the BGP table with a network statement.
Workaround: There are four possible workarounds:
 - 1) Use an “aggregate-address” configuration instead of the static route to generate the summary.
 - 2) Remove auto-summary from the BGP process.
 - 3) Enter the **clear ip bgp *** command.
 - 4) Remove and reconfigure the BGP network statement for the summary route.
- CSCsm36057
Symptoms: “Warning: error msgs in vc stats” messages are displayed continuously on the console.
Conditions: This symptom is observed when the router is reloaded.
Workaround: There is no workaround.

If any statistics are not being updated properly on the serial interfaces on the Ch-SPAs, enable the **debug hw sub slot/bay** command on the RP.

- CSCsm41303

Symptoms: A Cisco 12000 router with SIP-601 linecards may experience high CPU in the Tag Input process because of many packets being punted by the linecards to the PRP CPU. The packets are MPLS TTL expired packets that require an unreachable to be sent back. These packets should be processed on the linecard, but they are not.

Conditions: This symptom is observed only on SIP-601 10G linecards.

Workaround: There is no workaround.

- CSCsm43195

Symptoms: A configuration of L2VPN interworking between SIP-601/GE SPA to SIP- 401/CT3/FR DLCI switching and with a QoS egress policy applied on the SIP-601 GE SPA interface, traffic may propagate egress on the GE port.

Conditions: When the policy is not applied, traffic flows egress on the GE SPA based interface. When the policy is applied, no traffic is seen egress on the GE interfaces.

Workaround: There is no workaround.

- CSCsm48176

Symptoms: Line cards on a Cisco 12000 series router or a Cisco 7500 router might crash.

Conditions: This symptom is observed when the **no ip multicast- routing distributed** command for a VRF is issued when multicast tunnels are up. This symptom is also observed when MVRFs are deleted.

Workaround: Stop multicast traffic before deleting VRFs or issuing the **no ip multicast-routing distributed** command.

- CSCsm57369

Symptoms: On switchover, we see the overhead message appearing in config if we have not configured.

Conditions: This symptom is observed only if there is a switchover in RPR+ or SSO mode.

Workaround: Manually change the config to restore the previous config.

- CSCsm64491

Symptoms: Connecting SPA-4XCT3/DS0 SPAs back to back and executing the **hw-module subslot x/y reload** command causes the line card to crash.

Conditions: All the interfaces should be up and running. Note that this symptom occurs only because of the issue introduced by CSCsg96660; it is not seen otherwise without the image having the fix for CSCsg96660.

Workaround: There is no workaround.

- CSCsm66081

Symptoms: If a multilink interface has one end connected to a Cisco 12000 router with a CHOC12/DS1-IR-SC and the other end connected to a non-Cisco- 12000 router, then the multilink interface receiver, at the non-Cisco-12000 router side, may drop all received packets because of packet fragment loss or out-of-order.

Conditions: This symptom may occur immediately when the first member link comes back up again after all member links of the multilink interface have gone down.

Workaround:

1) Create a new multilink interface.

2) Move the member links from the current multilink interface to the new multilink interface.

- CSCsm75339
Symptoms: Tracebacks on mic-reload of SIP601.
Conditions: Mic-reload of SIP601 with CT3 SPA.
Workaround: Reloading the secondary RP should restore the out-of-sync ifindex tables.
- CSCsm82600
Symptoms: PRP-1 fails to boot after an OIR/power cycle. LEDs might show RPT SENT or RP RDY.
Conditions: This symptom is observed upon a power cycle after upgrading the mbus-agent-rom of the PRP.
Workaround: Use the upgrade mbus-agent-rom slot force command with an older version of Cisco IOS software in the active RP to downgrade the mbus agent ROM of the problem RP.
- CSCso21681
Symptoms: An output policy on an MFR interface disappears when the SIP 601 card is reset.
Conditions: Configure the service policy and apply it to the output of the MFR interface. Reset the SIP 601 card, and the service policy will disappear from configuration.
Workaround: There is no workaround.
- CSCso22730
Symptoms: Prefixes learned via IGP (ISIS) get assigned “imp-null” as the local label for them.
Conditions: The router has ECMP paths to uplink routers via POS interfaces. It runs ISIS as an IGP. There could be TE tunnel configured on the POS interface. And frequent interface flaps.
Workaround: There is no workaround. Clear the route or flap the interface to bring back the correct local label.
- CSCso25848
Symptoms: With an ingress E2 GigE line card and an egress E5 line card, packets are dropped in the egress line card with TX bad BMA buffer counts increasing.
Conditions: This symptom is observed when the ingress is E2 and the egress is E5.
Workaround: There is no workaround.
Further Problem Description: This issue is not seen with an E3/E5 combination or an E2/E6 combination.
- CSCso31508
Symptoms: CEF and hardware CEF for global default route are inconsistent. This may cause the default traffic to be sent through the wrong interface.
Conditions: This issue occurs under the following conditions:
 1. Global default should point toward the core.
 2. VRF default should be learned from the remote PE.Workaround: Enter the following command:
clear ip route 0.0.0.0 0.0.0.0
- CSCso32397
Symptoms: An unexpected reboot occurs because of a software-forced crash.
Conditions: This symptom is observed when changes are made in the policy map.
Workaround: There is no workaround.

- CSCso33290

Symptoms: L2VPN traffic on an MFR interface is unable to pass through FR/IETF encapsulation MPLS trunk. Furthermore, if this MFR interface is deleted and re-added, the following error messages are received.

```
SLOT 4:Mar 20 11:51:05.459 UTC: %SPA_CHOC_DSX-3-ERROR: Serial4/0/0/1:0: response
parsing failed for DLCI (601) provisioning SLOT 4:Mar 20 11:51:05.471 UTC:
%SPA_CHOC_DSX-3-ERROR: Serial4/0/0/1:0: response parsing failed for DLCI (602)
provisioning
```

Conditions: This symptom is observed after an MFR interface is deleted and re-added.

Workaround: There is no workaround.

- CSCso47485

Symptoms: The E4+ line card crashes continuously with the following output:

```
SLOT 1:Jan 19 02:06:09.559 UTC: %TX192-3-CPUIF: Error=0x40
rd 0x15 base 0x12 hdr 0x14 last 0x14 wr 0x14 insert 0x0 back 0x1 len 0x2474 cnt 0x0
```

Conditions: There is no exact trigger. But this symptom is observed when there are corrupt packets being sent from the ingress card under unknown circumstances.

Workaround: There is no workaround.

- CSCso65289

Symptoms: High CPU utilization is seen on a Cisco 12000 series Internet router caused by the “IPC Seat Manager” process.

Conditions: This symptom may be observed when the router is enabled with multicast distributed routing and has high scaled multicast configurations.

Workaround: There is no workaround.

- CSCso73511

Symptoms: Configure the line delay trigger at the line level in the Choc48 linecard as shown below.

Router# **sh run | b 1/0**

```
controller SONET 1/0
alarm-report lais
alarm-report lrdi
alarm-report sd-ber
sts-1 1 serial t3
```

Router# **conf t**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)# **controller sonet 1/0**

Router(config-controller)# **delay triggers line 10000**

Router(config-controller)# **do sh run | b 1/0**

```
controller SONET 1/0
alarm-report lais
alarm-report lrdi
alarm-report sd-ber
delay triggers report
sts-1 1 serial t3
```

Conditions: The serial interface should be UP and running.

Workaround: There is no workaround.

- CSCso74028

Symptoms: The local PE is sending graft messages even after receiving data from the remote PE on an MVPN network.

Conditions: This symptom is observed when the graft-ack messages are lost in transit (could be due to misconfiguration/ACL, etc.).

Workaround: Fix the misconfiguration so that graft-ack messages are forwarded as expected.
- CSCsq00167

Symptoms: 12000-SIP-401/501/601 has 8 MB of FSRAM with the fix CSCsm13564. But PLU and TLU adjacencies in the 12000-SIP-401/501/601 support up to 4 MB.

Conditions: If the hardware is supporting 8 MB of FSRAM, the PLU can have access to this 8 MB. But this is not happening.

Workaround: Identified through the code review of CSCsm13564. There is no workaround.
- CSCsq03170

Symptoms: An input service policy with only the class-default class shows no matches.

Conditions: This symptom is observed after a reload of Cisco 12000 series routers, Linecard Engine 3, with an ATM interface configured for ATOM, Port Mode.

Workaround: Move traffic and the configuration to another interface.
- CSCsq24258

Symptoms: An E0 OC3 CH does not give the option to configure sts-1 interfaces.

Conditions: This symptom is observed when loading a Cisco IOS Release 12.0(32) S11 image on the router.

Workaround: There is no workaround.
- CSCsq28627

Symptoms: CPU hogs are seen in a 1-port E3 channelized OC48.

Conditions: This symptom is observed when any of the following is done:

 - controller shut/no shut
 - mic reload <slot>
 - hw-mod slot <xx> shut/no shut
 - hw-module slot <xx> reload

Workaround: There is no workaround.
- CSCsq36270

Symptoms: CE-CE pinging is failing.

Conditions: This symptom is observed when E5 POS is imposition.

Workaround: There is no workaround.
- CSCsq49823

Symptoms: MDfS may get disabled in a scaled mVPN environment that has many global mroutes. Once disabled, it may keep on changing between the “active” and “disabled” states. Linecard CPU utilization may also go high.

Conditions: This symptom is observed with a Cisco IOS Release 12.0(32)S10 image.

Workaround: There is no workaround.

- CSCsq70534

Symptoms: A router crashes because of a block overrun (overwriting the memory block).

Conditions: This symptom is observed only when templates are exported in the export packet, which is used only in version 9 version of exporting.

Workaround: Version 5 could be used for exporting.

Resolved Caveats—Cisco IOS Release 12.0(32)S10

Cisco IOS Release 12.0(32)S10 is a rebuild of Cisco IOS Release 12.0(32)S. The caveats listed in this section are resolved in Cisco IOS Release 12.0(32)S10 but may be open in previous Cisco IOS releases. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCek49315

Symptoms: LC crashes due to a very high rate link flap.

Conditions: Occurred on different SPAs inserted on GSR routers running 12.0(32)SY1 when FEC is disabled on the remote end.

Workaround: There is no workaround.

- CSCek63384

Symptoms: A service policy is unexpectedly removed.

Conditions: This symptom is observed when you apply a service policy to a multilink interface and then the interface is reset.

Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, reconfigure the service policy after the multilink interface has been brought up.

- CSCsa87034

Symptoms: When you attempt to clear the routing table, the neighbor is brought down instead.

Conditions: This symptom is observed when you enter the **clear bgp ipv4 unicast *** or **clear bgp ipv6 unicast *** command, causing respectively the IPv4 neighbor or IPv6 neighbor to be brought down.

Workaround: There is no workaround.

- CSCsc70055

Symptoms: A Cisco 7200 series may crash when you perform a graceful OIR of a port adapter that is processing traffic.

Conditions: This symptom is observed mostly when the port adapter processes ingress traffic.

Workaround: Do not perform a graceful OIR. Rather, perform a manual OIR.

- CSCsc91735

Symptoms: CyBus errors may occur during an HA switchover, causing most VIPs to be disabled on a Cisco 7500 series.

Conditions: This symptom is observed when MLP Multilink interfaces are configured on channelized T3 (CT3) port adapters.

Workaround: Reload microcode onto all affected VIPs.

- CSCsd10762

Symptoms: The following traceback appears:

FIB-4-FIBNULLIDB: Missing idb for fibidb Virtual4 (if_number 54).
 Conditions: This symptom is observed when a router is reloaded.

Workaround: There is no workaround.

- CSCsd49670

Symptoms: After recovery from a network outage, some multicast traffic may be duplicated for a period of up to 15 seconds.

Conditions: Occurred on a Cisco 12000 with 5 Gigabyte Ethernet line cards and running Cisco IOS Release 12.0(32)S. The router was configured for Protocol Independent Multicast source specific mode (PIM- SSM).

Workaround: There is no workaround.

- CSCse04220

Symptoms: The BGP table version remains stuck at 1, and the router may crash.

Conditions: This symptom is observed when you enter the **clear bgp ipv4 uni *** command for IPv4 or the **clear bgp ipv6 uni *** command for IPv6. The symptom may also occur when you enter the **clear bgp nsap uni *** command for a network service access point (NSAP) address family.

Workaround: Enter the **clear ip bgp *** command to clear the sessions, purge the BGP table, and prevent the router from crashing.

- CSCsg19546

Symptoms: The standby RP may reload unexpectedly because of a Redundancy Facility (RF) synchronization error.

Conditions: This symptom is observed on a Cisco router that is configured for SNMP, dMPLP, and SSO.

Workaround: Do not configure SSO. Rather, configure RPR+.

- CSCsh13581

Symptoms: Engine 5 line card crashes when MPLS is unconfigured either globally or on a subinterface.

Conditions: Occurred on a router running Cisco IOS Release 12.0(33)S. The problem can be seen even with two node setup with explicit NULL configured. There should be at least three parallel paths with equal weight between the source and destination.

Workaround: There is no workaround.

- CSCsh16951

Symptoms: There is high CPU usage by the TAG process on the E4+ ingress line card.

Conditions: This symptom is observed when MPLS traffic comes in to the ingress E4+ and the MPLS configuration on the ingress interface is removed.

Workaround: There is no workaround.

- CSCsh31546

Symptoms: Applying L4 operators (used with an ACL) on many interfaces at the same time generates a traceback.

Conditions: There is no set procedure for generating the traceback. You must play around with the configuration to generate it.

Workaround: Configure the ACL batch by batch; for example, 20 to 30 interfaces at a time.

- CSCsh32191

Symptoms: Cisco 12000-SIP-601= with SPA-10X1GE running Cisco IOS Release 12.0(32)S2 in slots 3 and 5 both crash to software forced crash. Additional symptoms:

No logs may be seen other than “%RP-4-RSTSLOT: Resetting the card” - Crashinfo may not be generated

Events in the log:

```
SLOT 4:May 2 16:17:33.195: %GENERAL-3-EREVENT: Failed to delete TCAM entry -Traceback=
400310E4 40597080 40597914 40597A60 41345534 41349360 41354978 4136B774 41362BCC
41362E6C 41363190 413640A4 SLOT 4:May 2 16:17:33.195: %SYS-2-CHUNKFREE: Attempted to
free nonchunk memory, chunk 45E099A0, data B0D0B0D. -Process= "CEF LC IPC Background",
ipl= 3, pid= 90 -Traceback= 400310E4 400E07E0 405986CC 40597A6C 41345534 41349360
41354978 4136B774 41362BCC 41362E6C 41363190 413640A4
```

Conditions: Routers was configured for CE to PE is using EIGRP. Edge facing line card is E5

Workaround: Configure **no default-information in in the EIGRP section on PE, as shown in the following example:**

```
address-family ipv4 vrf VrfOne redistribute bgp 1800 network 172.16.0.0 network 172.20.0.0 no
default-information in no auto-summary autonomous-system 100 exit-address-family !
```

Further Problem Description: Router may display the following log:

```
SLOT 5:Jan 5 01:05:33 KST: %GENERAL-3-EREVENT: Failed to delete TCAM entry -Traceback=
40030EF8 40589CE4 4058A554 4058A6A0 4122D3D8 412314B0 41231694 4123C7F8 41253540
4124AA70 4124AD08 4124B02C 4124BF40
```

- CSCsh44940

Symptoms: Dynamic MAC re-write for port-channel causes around a 50-percent traffic drop.

Conditions:

A---LB1-----LB2-----LB3---B

1) Port-channel between LB2 and LB1 with two E5 members. Removed the member, whose MAC address is used for the port-channel, on both the routers. 2) Added the member back to the port-channel.

Traffic flows from B to A.

Workaround: Reload the microcode of the line card.

- CSCsh54862

Symptoms: MPLS TE tunnel does not come up completely after using **no shut** on the tunnel interface. This tunnel interface then goes down after about 10 seconds.

Conditions: Occurs because RSVP Path/Resv messages are lost between head-end and tail-end.

Workaround: Configure static ARP so that RSVP setup message is not dropped.

- CSCsh64365

Symptoms: A ping does not yield a 100-percent result after you have entered the **no set-overload-bit** for an IS-IS configuration.

Conditions: This symptom is observed on a Cisco 7200 series but is not platform-specific.

Workaround: There is no workaround.

- CSCsh75224

Symptoms: RP crashes in IFS code when a SSH or TELNET session is established while the switch is attempting to download a configuration.

Conditions: Occurs on a Cisco Catalyst 6509.

Workaround: There is no workaround.

- CSCsi07219

Symptoms: An Engine 3 4GE-SFP-LC= crashes by a Software Forced Crash after NetFlow-related configuration changes are made at the interface level. The crashes can occur from 30 minutes to several hours later.

Conditions: On a Cisco 12000 series Internet router that is running Cisco IOS Release 12.0(32)SY2 with a 4GE-SFP-LC=, NetFlow configuration changes at the interface level (Full NF or SNF) can trigger the crashes. This bug applies to NFv9.

Workaround: There is no workaround.

- CSCsi17519

Symptoms: An E5 line card fails to boot up after multiple retries.

Conditions: This symptom is observed only on faulty hardware.

Workaround: There is no workaround.

Further Problem Description: The root cause is bad hardware that causes TCAM parity errors during line card init. In this particular line card, when the parity error interrupt is generated during line card init, the line card is reset. If the interrupt comes after line card init, the line card is not reset. So, in general, if the card reports multiple TCAM parity errors, and they are not correctable, it may be better to replace the hardware.

- CSCsi83259

Symptoms: The MPLS labels for packets that are forwarded via CEF and MPLS over a BGP route may not match the labels in the BGP table.

Conditions: This symptom is observed on a Cisco RPM-XF-512 that runs Cisco IOS Release 12.4(6)T5 but is not platform-specific.

Workaround: Enter the **clear ip route** command for the prefix in the VRF.

- CSCsi93023

Symptoms: A MOD 48 line card gets stuck in the UP IOS state for more than 45 minutes after an RPR switchover.

Conditions: The line card is MOD 48 and contains two 2-port SPA-2XCT3/DS0. This is connected to another router with MOD 48 with two 2-port SPA- 2XCT3/DS0. This is a back-to-back connection with all the T1 links created on both the SPA-2XCT3/DS0. Both MLPPP and MLFR bundles are created with half of the T1 links assigned to MLPPP and the other half assigned to MLFR with traffic flowing in the links.

Under these conditions, when an RPR switchover is performed, the MOD 48 gets stuck in the UP IOS state and does not recover for 50 minutes. After this duration, it comes up automatically.

Workaround: There is no workaround. To recover immediately from this state, reload the card.

- CSCsi98730

Symptoms: The MPLS labels for packets that are forwarded via CEF and MPLS over a BGP route may not match the labels in the BGP table, which may lead to traffic loss.

Conditions: This problem occurs under certain circumstances and timing conditions.

Workaround: When the symptom occurs, enter the **clear ip route** command for the prefix in the VRF.

- CSCsj16016

Symptoms: With an ingress E2 GigE and an egress E5 (SIP 600/601 with a 1x10GE SPA), packets are dropped in the egress line card with TX bad BMA buffer counts increasing.

Conditions: This symptom is observed when the ingress is E2 and the egress is E5.

Workaround: There is no workaround.

Further Problem Description: This issue is not seen with an E3/E5 combination or an E2/E6 combination.

- CSCsj23805

Symptoms: Using the **show isis timers** causes the router crashes.

Conditions: Occurred on a router running Cisco IOS Release 12.0(31)S2y.

Workaround: There is no workaround.

- CSCsj59130

Symptoms: A router crashes when QoS is configured on POS and traffic line rate is sent.

Conditions: This symptom is observed when QoS and above line rate traffic.

Workaround: Remove QoS.

- CSCsj78019

Symptoms: Buffers on a line card are depleted, causing the LC to stop transmitting packets and possibly reset.

Conditions: E3/E5 on Tx side may have buffer depletion if running a defective image that corrupts the OQ to 0.

Workaround: Reload the line card.

- CSCsj88891

Symptoms: A console message is displayed with an unknown MPLS peer and VCID.

Conditions: This symptom is observed after the xconnect configuration is deleted.

Workaround: There is no workaround.

- CSCsk14495

Symptoms: A bogus line card crash is reported during a PLIM reset.

Conditions: This symptom is observed during a PLIM reset.

Workaround: There is no workaround.

- CSCsk15805

Symptoms: If you shut down a TE tunnel interface and you have a static route through the tunnel, the routing table is not updated immediately but only when the static scan runs (every minute by default).

Conditions: This problem is fine if the static route is pointing to a physical interface and happens only with TE tunnel interfaces when it is configured with the **ip routing protocol purge** command.

Workaround: Remove the **ip routing protocol purge** command or tune the adjust timer (**ip route static adjust-time** command).

- CSCsk30571

Symptoms: Field diagnostics fail (indicating a DOWNLOAD FAILURE) on the standby PRP2 when the PRP2 has 4 GB of memory installed.

After 40 minutes, the default download time limit, field diagnostics declare a download failure and reload the board. The failure message for this looks like the following:

Field Diagnostic: ****DOWNLOAD FAILURE**** while preparing slot {#}

Field Diag eeprom values: run 3 fail mode 5 (DOWNLOAD FAILURE) slot {#} last test failed was 0, error code 0 Shutting down diags in slot {#}
Board will reload.

Conditions: This symptom is observed for any release of Cisco IOS software when you attempt to run field diagnostics on a standby PRP that has 4 GB of memory.

Workaround: There is no workaround.

- CSCsk36276

Symptoms: Traceback seen at `tfib_post_table_change_label_request_needed`.

Conditions: Occurs during SSO switchover on a Cisco 7606 router.

Workaround: There is no workaround.

- CSCsk36552

Symptoms: Some packet flows may be dropped when the next-hop is load-shared between MPLS-TE tunnel and physical interface. The next-hop entry for the physical interface is invalid in Hardware-CEF table in ingress Line-Card during this problem. This cause the some packet flows which look up the invalid entry as the result of hash calculation to be dropped. The other flows which looks up the tunnel interface are not affected.

You can check the detail of hardware-CEF table for this problem by entering the **show ip hardware-cef prefix detail** command in Engine 3 and Engine 5.

Conditions: This problem occurs when the next-hop is load-shared between MPLS-TE and physical interface. This problem may be observed when using Engine 3 or Engine 5 as the ingress Line-Card on GSR.

Workaround: There is no workaround.

- CSCsk47914

Symptoms: Traffic forwarding stops after micro-reloading the egress card when E4+ is ingress.

Conditions: Occurs after micro-reload of the egress line card

Workaround: 1. Micro-reload the E4+ line card. 2. Use the **clear cef line card ingress card slot#** command to recover the traffic.

- CSCsk49843

Symptoms: E3 4xOC12 ATM line card may crash on enabling feature mode.

Conditions: Occurs when IPv4 VPN routing/forwarding (VRF) is configured on an IPv6-enabled interface.

Workaround: Apply an IPv6 ACL to “permit any any”.

- CSCsk71509

Symptoms: Line card stops forwarding after the **ip default-network 192.168.228.0** command is entered.

Conditions: Occurs on a LC Engine 5 with 12000-SIP-601 and running Cisco IOS Release 12.0(32)SY1 or 12.0(32)SY4. Problem also occurs on SPA-8XCHT1/E1 and 10Gigabit.

Workaround: Use Interior Gateway Protocol (IGP) to propagate the default route 0.0.0.0. BGP or OSPF also work. You can also add static route 0.0.0.0/0.

- CSCsk81155

Symptoms: OSPFv3 loses hello packets causing neighbors to flap.

Conditions: Occurs on a Cisco GSR router running Cisco IOS Release 12.0(32)S7 and later when TE tunnels are configured.

Workaround: There is no workaround.

- CSCsk81725

Symptoms: All E6 line cards are holding incorrect output slot information in hardware CEF for default route. At the same time, other E4+ and E2 LCs have no problem with hardware CEF.

Conditions: Unknown.

Workaround: Use the **clear ip route 0.0.0.0** command.

- CSCsk82701

Symptoms: Hot Standby Routing Protocol (HSRP) Virtual IP address is unreachable. IP address assigned to the interfaces is reachable.

Conditions: Problem was seen in GSRs with different SPAs. Problem occurs only when line card is installed for the first time or if it is moved between slots. Problem only occurs if the same interface is both configured for HSRP and assigned to VPN routing/forwarding (VRF).

```
interface GigabitEthernet3/0/0.5 ip vrf forwarding ip address X.X.X.2 X.X.X.X standby 1 ip X.X.X.1 standby 1 priority 110 standby 1 preempt
```

Workaround: Reload active and standby router as if you reload only active there is a chance standby router once become active may hit the problem. Or, remove the HSRP configuration before moving the line card.

- CSCsk83652

Symptoms: Ping from CE to PE fails

Conditions: Occurs when multilink bundle is removed from SIP 401/501/601/600 using **no multilink-group** and added to SIP 400/6CT3 LC/2CHOC3 LC.

Workaround: Use a new multilink bundle (multilink2) when removing member links from the SIP 401/501/601/600 (multilink1) and adding links from SIP 400 / 6CT3 LC / 2CHOC3 LC . It is not sufficient to delete the bundle (multilink1) and add the bundle configuration back with the same bundle name as it does not reset the layer 2 information.

- CSCsk99530

Symptoms: The MPLS forwarding table has an untagged outgoing entry for a VPNv4 prefix in a CSC case.

Conditions: This is an LDP/IGP (OSPF etc.) based CSC-PE. The VPNv4 prefix shall have a local/redistributed (PE-CE OSPF etc.) path as well as an iBGP path. If the CE path is toggled and then there is a LABEL ONLY change from the iBGP neighbor, the issue will be seen. BGP will end up programming “Untagged” for the local/redistributed prefix, overwriting what is given by LDP.

Workaround: There is no real workaround. To clear the problem, issue a **clear ip route** command for the vrf-prefix in question. If there are redundant paired PEs, make sure to clear the problem on both routers with the **clear ip route** command.

- CSCsl09752

Symptoms: Packet drops occurring on PE router.

Conditions: Occurs after sending traffic from VPN routing/forwarding (VRF). Traffic is stopped until the mroute entries get cleared. When traffic is sent from core, packets are dropped.

Workaround: Reload the line card.

- CSCsl11335

Symptoms: The number of entries obtained from the "ciscoMvpnBgpMdtUpdateTable" table using the **getmany** command is incorrect

Conditions: Occurred on a Cisco 7200 router running Cisco IOS version 12.4(17.9)T.

Workaround: There is no workaround.

- CSCs115026

Symptoms: Configuration applied to a multilink interface is not reflected on the interface.

Conditions: Occurs when a configuration is applied immediately after adding the first link to a multilink PPP or a multilink frame-relay bundle. It affects any configuration applied to the main interface or to the sub-interface of the bundle. The problem does not occur when adding subsequent member links to the bundle.

Workaround: After adding the first link, wait 15 seconds before applying any configuration to the bundle interface or on the sub-interface. If any of the configurations are missing, re-apply them.

- CSCs116385

Symptoms: Line card reloads.

Condition: Occurs after high-availability switchover and caused by excessive number of control messages.

Workaround: There is no workaround.

- CSCs117766

Symptoms: Attempting to configure serial interfaces results in the following message and a traceback:

```
%FIB-2-HW_IF_INDEX_ILLEGAL: Attempt to create CEF interface for Serialx/x with illegal index: -1
```

Conditions: When this happens the "ifindex" table appears to be incorrect on the PRP as a result of a race condition related to online insertion and removal (OIR) events. This problem should only occur if SSO redundancy is configured.

Workaround: If this happens on an HA-protected Active RP, check whether the Standby RP has good if- index values for all interfaces by running the **show idb EXEC** command on the Standby RP. If so, then do an RP switchover, so the RP with good interface indexes becomes the Active RP.

If the Standby RP shows this symptom, reload the Standby RP and check that after it comes up it has good if-index values, which should happen in most cases.

- CSCs132220

Symptoms: Cisco 12000 router running Cisco IOS Release 12SY may experience intermittent communications problems over Bridged VCs and ARP entries are not repopulated.

Conditions: Occurs when VC is configured for half-bridging and the router is running Cisco IOS Release 12.0SY.

Workaround: Use Cisco IOS Release 12.0S or, use VCs with routed encapsulation.

- CSCs133781

Symptoms: Primary RP crashes when the **clear counter** command is entered.

Conditions: Occurs when the command is entered while traffic is flowing.

Workaround: There is no workaround.

- CSCs141107

Symptoms: When explicit-null packets are received on URPF bundle, there is a possibility of BMA errors and crash.

Conditions: Occurs when explicit-null and URPF are configured.

Workaround: There is no workaround.

- CSCsl51587

Symptoms: The channelized SPA is in admin down state. When the **show hw-module subslot x brief** command is entered on the LC, the LC may crash.

Conditions: Unknown at this time.

Workaround: There is no workaround.

- CSCsl53811

Symptoms: Some FRR database entries become active after reoptimization. Traffic on the LSP which become FRR active is forwarded to the wrong path and continues to drop.

Conditions: This problem may happen when manual or timer reoptimization is performed during convergence. This problem may happen when “Tunnel head end item” and “LSP midpoint item” in FRR database have more than one entry in each item. This problem may happen when midpoint entry in “LSP midpoint item” is the LSP using “loose” path-option on a headend router.

Workaround: There is no workaround.

Further Problem Description: FRR database state and the traffic recover by doing primary tunnel or backup tunnel’s “shutdown” / “no shutdown” if this problem occur. If we configure longer reoptimization timer or we perform manual reoptimization after convergence, this problem may not occur

- CSCsl60370

Symptoms: GSR not soaking SLOS and bringing down interface immediately

Conditions: The issue occurs only when the GSR redundancy switchover happens.

Workaround: There is no workaround.

- CSCsl62276

The supplied note does not exist in CDETS

- CSCsl63885

Symptoms: Packet drops occur when doing MPLS ip2tag and tag2ip load balancing on an Engine 2 line card.

Condition: Occurs on a Cisco 12000 series router running Cisco IOS Release 12.0(32)sy2d.

Workaround: Enable LDP on the tunnel.

- CSCsl65264

Symptoms: EF CAR value does not set properly in TCAM for MFR bundle interface.

Conditions: Occurs when MFR interface is shut and no shut.

Workaround: Remove and re-apply output service policy to the MFR interface.

- CSCsl65977

Symptoms: IOS field diagnostics is failing with various error messages about “Slave Clock” such as displayed below:

```
Error disabling LC Enable register on CSC 0, SCA768_LC_ENABLE_2_S 0x7f, read_count 100
... Timed out waiting for TX Network Interrupt to happen ... Slot 16, Slave Clock
Control Register 0x00000000
```

Conditions: This has only been observed on a Cisco 12000 router when there are 12010E-CSC and 12010E-SFC fabric card in the chassis.

Workaround: There is no workaround.

- CSCsl67815

Symptoms: When core-facing line card reloads or has link flap, the edge-facing E5 for mVPN may not forward mVPN traffic.

Conditions: This defect is observed with an internal version off Cisco IOS Release 12.0(33)S.

Workaround: Enter the **clear ip mds line** *<edge facing E5 lc slot>* command.

- CSCsl81258

Symptoms: On a Cisco 12000 router running Cisco IOS Release 12.0(32)SY4, the SNMP ifIndex is missing for subinterfaces of the first SPA of a Engine 5 SIP-600 Line Card, as follows:

```
router#sh snmp mib ifmib ifindex GigabitEthernet15/0/3.951 Invalid ifIndex for
GigabitEthernet15/0/3.951
```

This issue affects accounting and billing.

Conditions: Occurred after router was upgraded from Cisco IOS Release 12.0.(31)s6 to Cisco IOS Release 12.0.(32)SY4.

Workaround: There is no workaround.

- CSCsl92482

Symptoms: Fragmentation is handled incorrectly on GSR E5 line card. We can send up to around 2Gbps of fragmented traffic without performance impact. When the egress line card CPU reaches 100%, the rate of the fragmented traffic drops down to 50Mbps.

Conditions: Occurs when all CPU resources of the egress LC are consumed.

Workaround: There is no workaround.

- CSCsl93926

Symptoms: E5 line card configured for CFI and BFI may crash when passing mVPN traffic.

Conditions: This is observed with Cisco IOS Release 12.0(32)SY5.

Workaround: There is no workaround.

- CSCsl98882

Symptoms: Traffic stops forwarding after the deletion of a security output ACL which is shared with the other port on a two-port OC-192, with the port carrying the traffic having a feature-output ACL.

Conditions: Occurs on a two-port OC-192 E6 card. Both the ports should be configured with output or input security ACLs, and one port which is carrying the traffic should have output or input ACL. For this issue to happen, all the ACLs need to be either output or input type simultaneously.

Workaround: Configure a new ACL with a different name from the original ACL, then remove it. The traffic can then be forwarded again.

Further Problem Description: This issue is specific to E6 alone and will not happen on E4.

- CSCsm02749

Symptoms: When multicast VPN routing/forwarding instance (mVRF) is un-configured, memory leak may occur in line cards.

Conditions: This symptom is observed in Cisco 12000 Series Routers and Cisco 7500 Series Routers when multicast distributed routing is enabled on VPN routing/forwarding instance.

Workaround: There is no workaround.

- CSCsm04631

Symptoms: RP crashes due to memory corruption.

Conditions: LC or SPA sending wrong VC number during stats update.

Workaround: There is no workaround.

- CSCsm11787

Symptoms: Customer reporting intermittent loss of L2 tunnel with no error messages.

Conditions: Occurs on a Cisco 7500 router running Cisco IOS Release 12.0(31)S02y.

Workaround: There is no workaround.

- CSCsm17607

Symptoms: GSP image not getting build

Conditions: Error in implicit declaration bfr_is_jag48_chocx_card.

Workaround: There is no workaround.

- CSCsm24189

Symptoms: 1choc12 ISE: PLIM might reset due to heartbeat failure.

Conditions: This happens when the following errors occur on the PLIM console: [2]T1:5 rx error(crc or non-integer size) 5 [2]T1:5 rx error(crc or non-integer size) 5

And when one or more paths have PAIS.

Workaround: Reduce the TEMUX logging level to 0 as follows **attach slot# plim logctl /dev/temux 0** And then clear the path AIS.

- CSCsm32438

Symptoms: The ifStackStatus results for SPA-4XCT3/DS0 on GSR intermittently do not show relationship between Serial interface and T1, nor T1 to CT3.

Conditions: Occurs when running Cisco IOS Release 12.0(32)S6d with SPA-4XCT3/DS0. Polling ifStackStatus results do show layered relationship with Serial interface, T1 to CT3.

Workaround: Remove and add again the T1 link channel-group if possible.

- CSCsm33743

Symptoms: VIP reloads.

Conditions: Occurs upon unconfiguring a service-policy from an interface. The crash is triggered by an illegal memory access operation. The issue can affect any interface and on any platform.

Workaround: No workaround.

Further Problem Description: This bug does not impact Cisco IOS Release 12.2SXF, 12.4, or 12.4T releases. This is seen very rarely and is not reproducible in lab.

- CSCsm45666

Symptoms: E5 LC crash on startup with multicast traffic flowing.

Conditions: Reboot the router.

Workaround: There is no workaround.

- CSCsm61527

Symptoms: Service policy with DCBWFQ does not offer guaranteed bandwidth.

Conditions: Occurs when DCBWFQ is configured in RSP router loaded with an internal version of Cisco IOS Release 12.0(32)S10.

Workaround: Increase the queue limit manually.

- CSCsm87206

Symptoms: Alternate PVC may go down if you reload the local PE line card 10 seconds after the remote PE line card.

Conditions: Occurs with Cisco 12000 router loaded with Cisco IOS Release 12.0(32)sy0i image. Local PE is configured with 4xCT3, and remote PE is configured with 1xSTM1 and L2tpv3.

Workaround: Reload with long delay between local and remote PE's LC

Resolved Caveats—Cisco IOS Release 12.0(32)S9

Cisco IOS Release 12.0(32)S9 is a rebuild of Cisco IOS Release 12.0(32)S. The caveats listed in this section are resolved in Cisco IOS Release 12.0(32)S9 but may be open in previous Cisco IOS releases. This section describes only severity 1, severity 2, and select severity 3 caveats.

Basic System Services

- CSCef32207

Symptoms: The **no snmp trap link-status** command is not available.

Conditions: Occurs only in the Frame Relay sub-interface.

Workaround: There is no workaround

- CSCsd59610

Symptoms: Cisco 7500 router with a RSP8 running Cisco IOS Release 12.0(27)S5b may experience traceback errors when the command **bgp regexp deterministic** is issued.

```
%SYS-4-REGEXP: new engine: regexp compilation had failed.
-Process= "BGP Router", ipl= 0, pid= 172
-Traceback= 40E601F4 40E5E8C0 40E5F950 40E5E128 4060BD4C 407CCF14 407CD440 407CE4A0
407A944C 407AB594 407ABE90 4079BA34
```

Conditions: Traceback appears after issuing the command **bgp regexp deterministic**.

Workaround: Disable **bgp regexp deterministic**.

- CSCse68904

Symptoms: IPC-INVALID with tracebacks seen after switchover.

Conditions: RPR-PLUS is configured on Cisco 7500 router.

Workaround: There is no workaround.

- CSCsg39295

Symptoms: Password information may be displayed in a Syslog message as follows:

```
%SYS-5-CONFIG_I: Configured from scp://userid:password@10.1.1.1/config.txt by console
```

Conditions: When using SNMP to modify a configuration by means of the CISCO-CONFIG-COPY-MIB, selection of ConfigCopyProtocol of SCP or FTP may result in the password being exposed in a syslog message.

Workaround: When using SNMP to modify a configuration by means of the CISCO-CONFIG-COPY-MIB, use the ConfigCopyProtocol of RCP to avoid exposure of the password.

- CSCsg69244

Symptoms: After you have performed a microcode reload on a router, a ping may not go through for 100 percent.

Conditions: This symptom is observed on a Cisco router that has an RSP after you have entered the **microcode reload** command.

Workaround: There is no workaround.

- CSCsj05318

Symptoms: The following error messages occur:

```
May 9 08:12:02.449: %CONTROLLER-5-UPDOWN: Controller E1 3/1/7, changed state to down
May 9 08:12:03.449: %CONTROLLER-5-UPDOWN: Controller E1 3/1/7, changed state to up
May 9 08:48:16.354: %CONTROLLER-5-UPDOWN: Controller E1 3/1/7, changed state to down
May 9 08:48:16.354: %RSP-3-ACCERROR: Serial3/1/7:1 acc E80002BA had bad value 39
-Traceback= 40348B24 404E4DEC 4050B378 405086B4 405087AC 4050CAAC 4050E754
```

Conditions: Possibly caused by unstable line 3/1/7.

Workaround: Shutdown the interface 3/1/7.

- CSCsj68341

Symptoms: snmpEngineBoots variable, used in SNMPv3 packets, not incremented correctly during RP switchover when using RPR+ on a Cisco 12000 Series router. This may cause issues for third party mediation devices that attempt to utilize this variable to decide if the SNMPv3 configuration needs to be reinstated after a reboot or RP switchover of the device.

Conditions: Add SNMPv3 configuration, then do an RP switchover two times. At least one of the times, the snmpEngineBoots variable will not have incremented. Variable can be decoded via packet capture of SNMPv3 packets from router, or with snmpwalk:

```
snmpwalk -v 3 -Os -u USERNAME -l authNoPriv -A PASSWORD Z.Z.Z.Z snmpEngineBoots
```

Workaround: There is no workaround.

- CSCsk03336

Symptoms:

Interface counters on E5 line cards may show incorrect packet input stats in the output of **show interface**.

Conditions: Problem is seen when the line card CPU spikes to over 90% due to the process “CEF LC IPC Backg”

Workaround: Issuing the **clear counters** command will temporarily correct the counters.

- CSCsk09044

Symptoms: Customer experienced excessive environmental messages on the logs when environmental temperature is still normal.

```
Jun 22 19:44:18.229: %CI-6-ENVNORMAL: RSP(6) Inlet measured at 19C/66F
Jun 22 19:44:21.765: %CI-6-ENVNORMAL: RSP(6) Hotpoint measured at
25C/77F
Jun 22 19:44:25.301: %CI-6-ENVNORMAL: RSP(6) Exhaust measured at
25C/77F
Jun 22 19:44:28.836: %CI-6-ENVNORMAL: RSP(7) Inlet measured at 19C/66F
Jun 22 19:44:32.372: %CI-6-ENVNORMAL: RSP(7) Hotpoint measured at
24C/75F
Jun 22 19:44:35.908: %CI-6-ENVNORMAL: RSP(7) Exhaust measured at
24C/75F
Jun 22 19:44:39.556: %CI-6-ENVNORMAL: +12 Voltage measured at 12.26
```

```
Jun 22 19:44:43.092: %CI-6-ENVNORMAL: +5 Voltage measured at 5.11
Jun 22 19:44:46.627: %CI-6-ENVNORMAL: -12 Voltage measured at -12.03
Jun 22 19:44:50.163: %CI-6-ENVNORMAL: +24 Voltage measured at 21.60
Jun 22 19:44:53.699: %CI-6-ENVNORMAL: 2.5 Reference measured at 2.47
```

Conditions: These are called ENVNORM clearances messages and indicate that a problem condition has returned to normal condition. Unless there is a problem condition these should not be seen and if once seen they should not repeat.

Workaround: There is no workaround.

EXEC and Configuration Parser

- CSCsj85585

Symptoms: Active is getting the following errors:

```
00:45:48: %IPCGRP-3-ERROR: set cfg-exited: timeout 00:46:11: %IPCGRP-3-ERROR: standby
set time: timeout
```

Conditions: If we give the any “do commands” under config mode/(interface) and If we wait until (exec-timeout 1) timer times out, we can observe these errors in active and also output of “do command” is displayed in standby.

Workaround: There is no workaround.

Interfaces and Bridging

- CSCsh31952

Symptoms: High number of input errors and ignores when locally switching traffic on a VIP6-80. Traffic coming in on a PA-2FE and out a PA-A6-OC3-SMI on the same VIP we will see input errors on the PA-2FE.

Conditions: Occurs on a Cisco 7500 series router with an RSP16 with VIP6-80s running 12.4 PA-2FE and PA-A6-OC3-SMI.

Workaround: There is no workaround.

IP Routing Protocols

- CSCsc67367

Symptoms: The **set ip next-hop in-vrf** *vrf-name* command does not work in conjunction with import maps.

Conditions: This symptom is observed on a Cisco router that is configured for BGP.

Workaround: There is no workaround.

- CSCsd72747

Symptoms: A OSPF router in a NSSA that summarizes an address will keep the summary learned via a neighbor router after using the **clear ip route *** command.

Conditions: Both neighbors are summarizing the same network in a NSSA area and are advertising it.

Workaround: Use the **clear ip ospf process** command.

- CSCsf02935

Symptoms: A router that is configured for OSPF Sham-Link and BGP redistribution may crash.

Conditions: This symptom is observed only in network topologies with OSPF routes that traverse two or more sham links. For example, the symptom may occur in a hub-and-spoke topology with sham links between the hub and two or more individual spokes. This symptom was observed on a Cisco 10000 series but may also occur on other platforms.

Workaround: There is no workaround.

- CSCsg16778

Symptoms: A router may reload when Border Gateway Protocol (BGP) neighbor statements are removed from the configuration.

Conditions: This symptom is observed in rare circumstances on a Cisco router when BGP neighbors are removed very quickly by a script at a much faster rate than manually possible and when a large BGP table is already present on the router before the script adds and removes the BGP neighbors.

Workaround: There is no workaround.

Further Problem Description: If you manually remove the BGP neighbors, it is less likely that the symptom occurs.

- CSCsg42488

Symptoms: In an MPLS VPN where OSPF is being used between PE and CE, if the BGP VPNv4 routes received over the VPN backbone are advertised by a Juniper device, OSPF Route-Type and OSPF Router-ID extended community may not be interpreted correctly. This may result in the PE redistributing the incorrect route-type via OSPF.

Conditions: - OSPF being used between PE-CE - BGP VPNv4 prefixes received from a Juniper device

Workaround: If it is possible to configure OSPF Route Type Extended Community/OSPF Router ID Extended Community type to be advertised by the Juniper device, then using the 0x8000/0x8001 would avoid this problem.

RFC4577 defines two encodings for Route Type and Router ID BGP communities that are used in VPN context:

OSPF Route Type Extended Community - 0x0306 or 0x8000 OSPF Router ID Extended Community - 0x0107 or 0x8001

Cisco uses the original encodings (0x8000 and 0x8001) when advertising routes over the VPN backbone and does not currently recognize the new types (0x0306 and 0x0107).

- CSCsg43140

Symptoms: A router may crash during the boot process and return to ROMmon.

Conditions: This symptom is observed on a Cisco router that is configured for BGP and that has VPNs configured.

Workaround: There is no workaround.

- CSCsh02161

Symptoms: A Route Reflector (RR) does not withdraw a prefix that redistributes itself even if this prefix is removed from the BGP table.

Conditions: This symptom is observed on a Cisco router that functions as an RR that advertises two of the same prefixes with different Route Distinguishers (RDs) when one of these prefixes redistributes itself and when the other prefix is a route that is learned from an RR client via iBGP.

Workaround: There is no workaround.

- CSCsh12493

Symptoms: After addition/deletion/modification of a VRF and the re-addition of associated configuration, it becomes apparent that the RIB is not being updated by BGP after reconvergence, and LDP neighborhood is reestablished. As the RIB is not updated, neither is CEF. While BGP VPNv4 has the correct information, the RIB is empty of remote PE VRF subnets, and CEF has a default entry.

Conditions: This symptom is observed on Cisco 12000 series router that is running Cisco IOS Release 12.0(32)S6.

Workaround: Can be recovered by clearing BGP session.

- CSCsi48304

Symptoms: After a reload, the following error message may be displayed if an OSPFv3 router redistributes large numbers of the external routes:

```
%OSPFv3-3-DBEXIST: DB already exist
```

No impact to the operation of the router has been observed.

Conditions: Redistribution is configured, then router is reloaded.

Workaround: There is no workaround.

- CSCsj32013

Symptoms: A Cisco 12000 series router may crash unexpectedly.

Conditions: Occurred only on Cisco IOS Release 12.0(32)SY0f.

Workaround: There is no workaround.

- CSCsk35970

Symptoms: Repetitive CPU spikes are seen on Cisco 12000 series router, running 12.0(32)S and configured for BGP multipath with several iBGP and eBGP peers.

Conditions: TblVer is incrementing every 5 minutes, thus causing the BGP Router process to inflict CPU spikes at every 5 minutes.

Workaround: There is no workaround.

ISO CLNS

- CSCee04303

Symptoms: A Cisco router running ISIS routing protocol may experience spurious memory access issue. The following messages can be seen:

```
*Sep 5 10:40:11.781 JST: %ALIGN-3-SPURIOUS: Spurious memory access made at 0x61081F84
reading 0x4
*Sep 5 10:40:11.781 JST: %ALIGN-3-TRACE: -Traceback= 61081F84 610833C0 61083D8C
6108438C 610748D0 610751B4 00000000 00000000
```

Conditions: Occurs only while rebooting.

Workaround: There is no workaround.

- CSCee73764

Symptoms: The interface command **isis metric xxx** on the MPLS tunnel interface is not shown in the configuration, nor does it take effect when a non-default value is configured.

Conditions: When MPLS TE tunnel is configured and ISIS is used as routing protocol.

Workaround: There is no workaround.

- CSCsh38140

Symptoms: CEF drops seen when new link comes up, and IS-IS picks the new link as the best path.

Conditions: Only seen when IS-IS the IGP routing protocol used. The problem is that IS-IS is not an IP based routing protocol, so IS-IS does not depend on IP connectivity between the routers, and can install routes with a next-hop for which no ARP entry exists yet. This leads to a short window of loss until the ARP entry is resolved.

Workaround: Ensure the ARP entry is present, for example:

- Use static ARP entries for the neighboring routers.
- Enable an IP based protocol between the 2 routers, for example BFD.

- CSCsi25729

Symptoms: BFD is not enabled.

Conditions: Occurs when BFD is configured along with ISIS

Workaround: Reload the LC.

- CSCsj53361

Symptoms: IS-IS adjacencies may flap after a stateful switchover (SSO) has occurred.

Conditions: This symptom is observed when there are large number of adjacencies (for example, 16) and when the IS-IS database is large (for example, one LSP containing 5000 routes).

Workaround: Increase the hold time that is advertised in the IS-IS Hello (IIH) packet by entering the **router isis nsf advertise holdtime 90** command on the router on which the SSO occurs.

- CSCsj72039

Symptoms: The prefix of a serial interface that is configured for PPP or HDLC and that functions as a passive interface for IS-IS may not be installed in the local IS-IS database.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(18)SXF6 but is not release-specific.

Workaround: Remove and reconfigure the **passive-interface** command.

First Alternate Workaround: Enter the **clear isis *** command.

Second Alternate Workaround: Enter any command that triggers the generation of the local IS-IS database.

- CSCsj89636

Symptoms: For routers with parallel links connected through switches, if neighbor shuts down ethernet interface, ISIS routes in the routing table use that interface as nexthop will not be deleted even after it receives new LSP from the neighbor reflecting the topology change until adjacency times out, thus create temporary blackhole and delay the convergence.

Conditions: Parallel link exists between routers.

Workaround: Enable BFD on interfaces.

- CSCsk02919

Symptoms: IPV6 Traffic is hit in one direction after resuming when OIR is performed on the connecting SIP on the router at the other end.

Conditions: Topology in which the bug was found:

CRS1(GigE)------(GigE)GSR

Occurs when an OIR is performed on GigE Line Card of CRS1 connecting to the GigE of GSR the IPV6 traffic going in one direction (from GSR to CRS) is hit again for about 4 seconds after the traffic has resumed after the OIR.

Workaround: There is no workaround.

- CSCsk95829

Symptoms: A quick **shut/no shut** (less than 3 sec) of a traffic eng tunnel interface results in the tunnel being removed from the routing table.

Conditions: Occurs on a Cisco 7600 series router running Cisco IOS Release 12.2(33)SRB1. Routing protocol is ISIS.

Workaround: Wait at least 7 seconds to do the **no shut** after the initial **shut** on the tunnel interface. If you can not wait for than 7 sec to **shut/no shut** the tunnel interface then you can configure: **.ip routing protocol purge interface**

- CSCsk98772

Symptoms: Route might be missing in the routing table.

Conditions: If there is a DR change and ISIS SPF finishes before neighbor sends the router with correct LAN ID reflecting the new DR.

Workaround: Anything that can trigger another SPF run will correct this problem.

Miscellaneous

- CSCdv70397

Symptoms: Whenever an ACE is deleted on the RP from a numbered extended or standard ACL, the corresponding ACL is removed from the LC.

Workaround: Use one of the following:

1. Use named extended or standard ACLs.
2. If it is really necessary to use numbered ACLs, modify them offline, delete the whole ACL and re-apply it on the RP.

- CSCek56415

Symptoms: The Hierarchal Queuing Framework (HQF) is not removed after you have removed a service policy.

Conditions: This symptom is observed on a Cisco 7200 series that has an NPE-G1 and that runs Cisco IOS Release 12.2SB.

Workaround: There is no workaround.

- CSCek78719

Symptoms: While running a Cisco IOS Release 12.0(32)S image, an Engine 3 line card on a Cisco 12000 series router may report some CPUHOG error messages similar to the following:

```
%SYS-3-CPUHOG: Task ran for 2264 msec (282/155), process = Per-Second Jobs, PC = 400FC51C. -Traceback= 400FC524 400ACC0C 40102FCC 400ACC38 400D7580 400D756C
```

Conditions: This symptom happens during normal operation.

Workaround: There is no workaround.

- CSCin97669

Symptoms: The standby RP resets continuously because of synchronization failures.

Conditions: This symptom is observed on a Cisco router when you first perform an OIR of a VIP in which a port adapter is installed that supports both T1 and E1 (for example, a PA-MC-8TE1+ port adapter) and then an SSO switchover occurs.

Workaround: There is no workaround. You must power-cycle the standby RP to enable it to come up.

- CSCin98630

Symptoms: When an InARP request is received on an AAL5SNAP PVC, the router does not respond with an InARP reply.

Conditions: This symptom has been observed when the source address contained in InARP request is not in the subnet of the sub-interface on which PVC is configured.

Workaround: There is no workaround.

- CSCir02303

Symptoms: InARP map gets deleted and ping does not work.

Conditions: This problem is seen when there is P2P on one side and multipoint on the other. The map is deleted on the multipoint side, and the inARP configuration is changed on P2P side.

Workaround: There is no workaround.

- CSCsa83219

Symptoms: Configuring an SDCC interfaces on a 2xOC48 POS SPA on the Cisco 12000 Series platform causes the router to display the following error message.

```
%EELC_QOS_RES_MGR-3-HW_IDB_INDEX_TO_TX_PORT_MAPPING_FAILED:
Mapping of hwidb_index to tx_port failed. hwidb_index = 5"
```

The message is displayed every time an SDCC interface is configured for this SPA. There is no other adverse effect other than the message being displayed.

Conditions: This symptom is observed on a Cisco 12000 series router that is running Cisco IOS Release 12.0(32)S.

Workaround: There is no workaround.

- CSCsc45827

Symptoms: T1/e1 stay up when BERT is running.

Conditions: BERT once started, cannot be stopped.

Workaround: Reload the SPA.

- CSCsd97412

Symptoms: LC gets reset.

Conditions: SPABRG generates excessive interrupts.

Workaround: There is no workaround.

- CSCse34197

Symptoms: Ping fails to remote CE.

Conditions: This symptom occurs after edge interface on a PE is micro reloaded, for example 4t3/e3 serial interface with PPPoMPLS AToM circuit.

Workaround: Try one of the following workarounds:

1. Reload the SPA.
2. Remove and reapply xconnect configuration.

- CSCse85151

Symptoms: Cisco Catalyst 4500 Supervisors and Cisco Catalyst 4948 that are running Cisco IOS Release 12.2(31)SG crash when one of the following commands are issued:

- **show buffers all** - **show buffers assigned** - **show buffers input-interface**

Conditions: This symptom occurs when one of the following commands is issued:

- **show buffers all** - **show buffers assigned** - **show buffers input-interface**

Workaround: Do not use any of the above commands. For troubleshooting high CPU issues use the steps indicated in the following tech tip instead:

http://www.cisco.com/warp/public/473/cat4500_high_cpu.html

- CSCse92201

Symptoms: The following traceback is observed:

```
SLOT 2: Aug 31 21:41:09.908: %SW_MGR-3-CM_ERROR: Connection Manager Error - provision
segment failed [ADJ:FR:1774000] - no interface available.
-Traceback= 6010C364 6010C8C0 60819570 60819610 60781D4C 608171E0 60829C4C 60829D0C
60817A9C 60817C2C 6080A4B0 60829C4C 60829D0C 6080B058 60806A30 608098E4
```

Conditions: Reload the router.

Workaround: There is now workaround.

- CSCsf97715

Symptoms: When both ACL and SNF are configured on one 3GE-GBIC-SC, SNF cannot work, and the CPU usage is high.

Conditions: This problem appears in Cisco IOS Release 12.0(28.4)S1 and is not seen in previous releases.

Workaround: Keep only one feature on the LC or downgrade IOS.

- CSCsg86567

Symptoms: When reloading a Cisco 7500 router (lsnt-ap-pe) with Cisco IOS Release 12.0(32)S5, several IDBINDEX_SYNC-3-IDBINDEX_ENTRY_LOOKUP and tracebacks occur in the standby log.

Conditions: This symptom has been observed on a Cisco 7500 router platform with MVPN configured.

Workaround: There is no workaround.

- CSCsh20034

Symptoms: IPv6 traffic drops (in 6PE scenario) on PE (core facing interface). IPv6 version errors are also seen.

Conditions: This symptom is seen in Engine3 line card. This issue is seen in Cisco IOS Release 12.0(33)S and Release 12.0(32)SY2 images.

Workaround: Use the **hw-module reload** command.

- CSCsh51418

Symptoms: The following message may be seen on manual RP switchover in SSO mode:

```
%FM-2-BAD_TLV: Error in internal messaging - bad tlv 0
```

Conditions: This is Observed on Cisco 12000 series router with SSO S/w and IPv6 ACL(with Traffic).

Workaround: There is no workaround.

- CSCsh51580

Symptoms: On the E3 line card “non channelized 4 port OC12 -- 4OC12X/POS” when an IPv6 ACL is applied on an outgoing interface to match on “Routing” extension header, it will instead match on “Fragments” extension header.

Conditions: The same behavior is seen on E3 line card “Channelized OC12 CHOC12” on both incoming and outgoing interface.

Workaround: Match on “Routing” extension header, or match on “Fragments” extension header.

- CSCsh51907

Symptoms: The following may be seen on physical OIR of a SPA-4XT3/E3 from a SIP-501 linecard:

```
%SPA_PLUGIN-4-LED_WRITE: SPA-4XT3/E3[8/2]: LED write failed for port 1, status 3.
```

Conditions: This symptom is observed on a Cisco 12000 series router that runs the c12kprp-p-mz image of Cisco IOS Release 12.0(32)SY2

Workaround: There is no workaround

- CSCsh88212

Symptoms: BGP Neighbor drop after receiving a high rate of MCAST traffic without previously defined state.

Conditions: 100K PPS of Mcast arriving at input interface on a GSR E5 card causing neighbor loss.

Workaround: There is no workaround.

- CSCsi01578

Symptoms: The MAC address on standby are 0 in RPR+.

Conditions: This symptom has been observed when doing RPR+ switchover. The traffic is lost.

Workaround: No workaround.

- CSCsi30873

Symptoms: VIP crash is seen with dLFloLL and QoS config on MCT3

Conditions: Occurs when using **shut/no shut** on a multilink interface through which traffic is flowing. Also occurs when **clear interface multilink #** command is issued.

Workaround: There is no workaround.

Further Problem Description: IPv6 Traffic is dropping in IPv6-IP tunnel with E2,E3,E4, E5 cards

- CSCsi69192

Symptoms: Upon an RPR+ switchover on a PE router followed by a switching of core traffic to an auxiliary interface, some mroutes may not resume traffic.

Conditions: This affects E3 line cards. Line card is core for one vrf and edge for the other

Workaround: There is no workaround.

- CSCsi89068

Symptoms: A channelized STM-1 port adapter is not transmitting equal traffic compared to a Multichannel T1/E1 port adapter when links from both port adapters are part of the same multilink interface.

Conditions: The problem is seen under heavy load on the multilink PPP bundle with or without multilink fragmentation enabled.

Workaround: Place all member links from the bundle on the same type of port adapter.

- CSCsi89149

Symptoms: After a microcode reload of SPA-1XCHSTM1/OC3 has been executed, the sequence of interfaces as it appears in **show run** and **show ip interface brief** is changed.

Conditions: SPA-1XCHSTM1/OC3 is configured on an E5 Line Card. When the router is reloaded and the SPA-1XCHSTM1/OC3 is configured for the first time, the sequence in which the interfaces appears fine. However, when the microcode reload is executed on the LC, the sequence in which the interfaces are displayed is not as expected. It has no other known side effects. Specifically this does not affect the traffic, nor the SNMP interface indexes.

Workaround: Avoid reloading the LC.

- CSCsj07189

Symptoms: Using **snmpget** of an OID using the ifindex value of an interface for its index will result in an error:

```
snmpget -c <community> -v1 <device>
IF-MIB::ifDescr.92 Error in packet
Reason: (noSuchName) There is no such variable name in this MIB.
Failed object: IF-MIB::ifDescr.92
```

Conditions: This can occur after PAs have been swapped.

Workaround: Use **snmpwalk** to retrieve the IF-MIB values.

- CSCsj12728

Symptoms: Connect the TGN to one of the interface of OC48 SPA. Inject the PAIS alarm and check whether it is reported or not using command the **show controller pos x/y/z**. Then clear the alarm, immediately after this we can see B3-TCA alarm declared and cleared.

Conditions: The SPA interfaces should be up.

Workaround: There is no workaround

- CSCsj17694

Symptoms: Add/remove of MLPP interface can cause mod48 to crash.

Conditions: This is observed with Cisco IOS Release 12.0(32)SY image.

Workaround: There is no workaround.

- CSCsj19308

Symptoms: MLPPP/MLFR ping failure on SPA-2/4CT3 or SPA-CH-STM.

Conditions: MLPPP/MLFR configured on SPA-2/4CT3 or SPA-CH-STM.

Workaround: Reload the SPA using the **hw-module subslot <slot>/<subslot> reload**.

- CSCsj32904

Symptoms: When the **no bert** command is issued to remove a configured bert test before the timer has expired, the bert test may be reset and the slave RSP may also reset

Conditions: Seen in rsp-k4pv-mz-eng-sp.120-31.S2_V2

Workaround: Do not issue **no bert**, instead change the interval in the bert pattern to 1 and let the test time out naturally. Example: **bert pattern 2^20-O153 interval 1**

- CSCsj37071

Symptoms: All E1 interfaces on a PA-MC-E3 port adapter may flap continuously even after the traffic has been stopped.

Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that have a PA-MC-E3 port adapter when you configure 16 or 128 channel groups on each time slot (that is, time slots 1-31) and then generate traffic just above line rate traffic through all the channel groups. Note that the symptom is not platform-specific.

Workaround: Stop the traffic and reset the E3 controller of the PA-MC-E3 port adapter.

- CSCsj39711

Symptoms: Configuration of “hw-module slot x team compile acl no-merge” is missing after OIR of E3 POS card.

Conditions: OIR of POS E3 line card.

Workaround: Enter the command again.

- CSCsj47271

Symptoms: The following error message appears while removing an MFR bundle interface:

```
%FIB-2-IF_NUMBER_ILLEGAL: Attempt to create CEF interface for MFR1 with illegal
if_number: 0
```

Conditions: The error occurs if the MFR bundle interface is removed without removing the member links from the bundle.

Workaround: Remove the MFR bundle, wait approximately 1 minute, then re-add the configuration for the affected MFR bundle.

- CSCsj47347

Symptoms: Using CLI to delete a child policy on a Cisco 7500 series router causes the VIP to crash.

Conditions: The router has a hierarchical QoS policy attached to an interface. Traffic is flowing through the QoS policy. There are BGP updates happening on the router. The **no policy-map** command is executed to delete the child policy. The router is running Cisco IOS Release 12.0(32)S6.

Workaround: There is no workaround.

- CSCsj50513

Symptoms: All LCs goes to WAITRTRY state

Conditions: SFC is shut and one LC through which traffic is coming is shut.

Workaround: Reload the router.

- CSCsj52025

Symptoms: On enabling/disabling mcast hw-acceleration, the following error occurs:

```
1d06h: %REDUNDANCY-3-CONFIG_SYNC: Active and Standby lbl configuration out of sync"
message may be thrown.
```

Conditions: rpr-plus, enabling/disabling mcast hw-acceleration.

Workaround: There is no workaround.

- CSCsj52280

Symptoms: Using the **pos ais-shut** configuration may be lost on E3 POS linecard

Conditions: Occurs when following OIR or shutdown of card.

Workaround: There is no workaround.

- CSCsj52296

Symptoms: After changing redundancy mode via SNMP on GSR redundancy mode description is missing on SNMP O/P.

Conditions: Only on changing redundancy mode, this does not affect the functionality

Workaround: There is no workaround.

- CSCsj58716

Symptoms: Traffic drops occur on egress SIP-X01 interface during congestion.

Conditions: The problem occurs when egress is any SIP-X01 card and there is congestion on the outgoing interface and no default queue-limit is configured explicitly for the traffic class.

Workaround: The problem does not occur when a low limit is configured on the class and WRED is also configured.

- CSCsj62100

Symptoms: The **show controller psar frfab packet_dump** command has no effect.

Conditions: This command is used to capture corrupt packet data when assembler RP detects it.

Workaround: There is no workaround.

- CSCsj62309

Symptoms: Unexpected flows are seen on a GSR configured with aggregate netflow and acting as a provider edge router (PE). The unexpected flows is seen in the output direction of the CE-facing interface (vrf interface).

Conditions: When traffic is generated (FTP, UDP, ICMP), we can observe strange flows of IP precedence 5 (TOS A0). If there is no traffic flowing through, then the flows are not seen. The router runs Cisco IOS Software 12.0(32)S6. Both ingress and egress linecards are ISE Engine 3 linecards. The P-facing interfaces are bundled in a port-channel.

Workaround: There is no known workaround and this impacts customer billing.

Further Problem Description: The flows can be seen through the following command:

```
clk15ra#execute-on slot 3 sh ip cac ver flow agg as-tos | i Gi3/1.999 ===== Line
Card (Slot 3) ===== Gi3/1.999 0 PortCh1 0 00 64 121K 46 147.2 Gi2/0 0 Gi3/1.999* 0
00 96 238K 1300 144.6 Gi2/0 0 Gi3/1.999* 0 A0 76 3996 442 115.8 >>> Unexpected
```

- CSCsj65683

Symptoms: Wrong channel group obtained from the CLI.

Conditions: Occurs when BERT is run on a channel group.

Workaround: There is no workaround.

- CSCsj65713

Symptoms: Following unknown trigger events, a GSR running Cisco IOS version 12.0(32)S6 may not properly classify PIM MDT-encapsulated multicast traffic via an MQC queueing policy attached to a POS interface on an E3 POS linecard [4OC3X/POS-IR-LC-B=]. This symptom can be observed via executing the **show policy-map interface POS X/Y** command while multicast traffic with non-zero IP Precedence or DSCP Value is exiting the interface.

Conditions: The issue is observed on MDT encapsulated GRE multicast tunnel packets on a P router in an MPLS core. The P router's failing Line-Card is 4OC3X/POS-IR-LC-B= and the P router is running Cisco IOS version c12kprp-p-mz.120-32.S3.

Workaround: There is no workaround.

- CSCsj66400
Symptoms: Tracebacks and error messages seen on E2 POS LC when changing from the encaps from FR-HDLC encaps
Conditions: Occurs when unconfiguring the Frame-relay interfaces to the default encaps HDLC.
Workaround: There is no workaround.
- CSCsj68219
Symptoms: Tracebacks and error messages are seen.
Conditions: Occurs when configuring SR APS.
Workaround: There is no workaround.
- CSCsj72032
Symptoms: COPP fails after LC is reloaded.
Conditions: Occurs when LC should be reloaded.
Workaround: There is no workaround.
- CSCsj72234
Symptoms: The standby crashes when the 3-port Gigabit ethernet card is in admin down state after a switchover has happened
Conditions: The 3 port Gigabit Ethernet Card has to be in admin down mode and then 2 switchovers need to be done to get into this situation.
Workaround: Use the **no hardware-module slot <x> shut** command on the LC and admin shut it again.
- CSCsj74724
Symptoms: When the router is in transit mode (SRP shut down), the **show controllers** command will behave as follows:
 - LOS, LOF, and RDI signals are reported as if the SRP interface were up
 - Active defects are detected properly (SLOS SLOF PLOP) as if the SRP interface were up
 - Active defects will not get cleared even if the issue goes away until the SRP is brought up
 - FEBE messages are not reportedConditions: Occurs on a Cisco 10720 Router with SRP card in shutdown mode.
Workaround: Use **no shut** command on the SRP interface without assigning it an IP address.
- CSCsj77669
Symptoms: GRP may crash continuously on reload if a MFR interface in the router has **bfd neighbor command** configured.
Conditions: Occurs when **bfd neighbor** command is configured on MFR interface.
Workaround: Issue **send brk** from “telnet>” prompt and boot the router with a boot image. Then remove the “bfd neighbor” config from MFR and reload the router with the regular image.
- CSCsj77998
Symptoms: BFD sessions do not come up on Cisco ISR routers.
Conditions: BFD sessions remain in down state and do not transition to up state on Cisco ISR routers.
Workaround: There is no workaround.

- CSCsj86839

Symptoms: Field diagnostics for a card such as the SIP-401, SIP-501, SIP-601 fails with messages:

```
"Timeout waiting for Field Diag individual test completion
Field Diagnostic: ****TIMEOUT FAILURE**** slot 4: first test failed: 163,
SPA LPBK damsl, error 0
Field Diag eeprom values: run 44 fail mode 3 (TIMEOUT FAILURE) slot 4
last test failed was 163, error code 0
Shutting down diags in slot 4"
```

Moreover, depending upon which verbosity and debugging flags are enabled you may see a series of messages such as:

```
"Field Diag Misc Services requested for a slot (4) not in Field Diag mode, dropping
request."
```

This occurs until the slot is reloaded with the command **hw-module slot # reload**

Conditions: This problem occurs when field diagnostics is run on the SPA, “SPA-10x1GE” residing in any Jacket card.

Workaround: There is no workaround.

- CSCsj87371

Symptoms: In case that MPLS Traffic Engineering Tunnel (TE Tunnel) and Fast Reroute (FRR) are configured on 12000 Series router, FRR backup Tunnel does not restore MPLS LDP/TDP encapsulating packets inputting from Engine 4 Line Card.

Conditions: When Next hop is Head-end LDP/TDP over TE Tunnel and FRR become active, the labeled packets are not protected by the backup TE Tunnel so it causes continuous packet drop until new path is installed.

Workaround: There is no workaround.

- CSCsj89407

Symptoms: The tx-ring-limit value configured in PA-2CT3 may reset to its default value.

Conditions: Occurs while doing soft OIR of PA-2CT3.

Workaround: There is no workaround.

- CSCsj90463

Symptoms: Holddown timer value is different in “show bfd nbr detail” and “show bfd neighbor”. The detailed output of “show bfd neighbor” command displayed holddown timer value for async mode where as the summarized output showed the holddown timer value for echo mode. Change had to be made to have holddown field in both summarized and detailed output of “show bfd neighbor” to display same value.

Conditions: When holddown value in “show bfd summary” and “show bfd neighbor detail” are compared.

Workaround: There is no workaround.

- CSCsj91286

Symptoms: This issue is a traceback seen on boot when upgrading or downgrading an image. The traceback seen is:

```
'%MBUS_C2W-3-SPA_UNKNOWN_C2W_DEVICE: cannot find SPA's C2W device for slot:', and
running config for all SPA's may be lost from an engine 5 card.
```

Conditions: This issue is due to the Mbus Agent ROM and Mbus Agent RAM.

Workaround: Copy the startup configuration to the running configuration.

- CSCsj93388

Symptoms: 12000-SIP-501 reloads with the following error message:

```
%RP-3-FABPINGTIMEOUT: Fabric ping timeout
```

Conditions: This problem is seen when executing the following commands

```
Router#attach <slot number>
LC-SlotX>show controllers tofab queues outputq 0 2303 drr
```

Workaround: Enter valid queue numbers for “start_q” and “end_q” values in the command. Valid Queues are as follows.

- 0 - 2047 (Low Priority ToFab Unicast Queues)
- 2048 - 2055 (ToFab Multicast Queues)
- 2176 - 2191 (High Priority Tofab Unicast Queues).

The problem is not seen when DRR information is read for valid queues.

- CSCsj94561

Symptoms: A router may crash because of a bus error when you perform an OIR of a PA-MC-8TE1+ port adapter or when you enter the **hw-module slot slot-number stop** command for the slot in which the PA-MC-8TE1+ port adapter is installed.

Conditions: This symptom is observed on a Cisco 7200 series.

Workaround: There is no workaround.

- CSCsj97877

Symptoms: When E4P is egress and policing is configured in the policy, matching ip prec did not match labelled packets and matching exp did not match pure IP packets.

Conditions: When E4P is egress and policing is configured in the policy, matching ip prec did not match labelled packets and matching exp did not match pure IP packets.

Workaround: Match exp for labelled packets and ip prec for pure IP packets.

- CSCsj98594

Symptoms: SIP-600/601 LC reloads.

Conditions: Occurs on slow path.

Workaround: There is no workaround.

- CSCsj98725

Symptoms: The following traceback occurs when some policy/class addition/deletion or interface flaps is done:

```
SLOT 2:Jan 25 19:13:34 UTC: ee192_tx_q_cleanup_guts(): EE_QM_QOS_INTERNAL_ERROR
```

Conditions: It happens when some policy or class addition/deletion or interface flaps is done.

Workaround: Reload the LC to bring the LC-Resources to normal state.

- CSCsj98774

Symptoms: When changing the APS mode using **aps unidirectional** or **no aps unidirectional** the following error message may be seen:

```
%SONET-4-APSM: SONET9/0 (grp 1 chn 0: ACTIVE): APS mode mismatch - switching to unidirectional mode
```

Conditions: This problem is seen on a Cisco 12416 Internet Series router containing dual channelize OC-48 line cards configured for automatic protection switching. The router is running Cisco IOS Release 12.0(32)S6q.

Workaround: There is no workaround

- CSCsk02675

Symptoms: RP crash occurs.

Conditions: Occurs when cef linecard is cleared concurrently with the unprovisioning of the multilink bundle.

Workaround: Do not clear cef linecard and unprovision the bundle at the same time.

- CSCsk05059

Symptoms: A spurious access error occurs in `tfib_post_table_change_sanity_check()` function.

Conditions: This symptom occurs if route is deleted. `ROUTE_DOWN` event is triggered in `tfib_post_table_change()` function which in turn calls `tfib_post_table_sanity_check()`. In that function, spurious access is reported, as the only path of route is down.

Workaround: There is no workaround.

- CSCsk06322

Symptoms: "%REDUNDANCY-3-CONFIG_SYNC: Active and Standby lbl configuration out of sync" message may be seen on hw-module shut of spas

Conditions: This is a timing issue and does not occur with debugs enabled.

Workaround: This does not impact service, and there is no workaround.

- CSCsk08317

Symptoms: Hardware CHEF entry on line card is incorrect. Incorrect slot is observed by **show hip hardware-clef** command.

Conditions: The problem occurs on Engine4+ Line Card of Cisco12000 router. The prefix has two next hop with load balancing.

Workaround: Use the **clear hip route <prefix>** command to correct the problem.

- CSCsk08440

Symptoms: E4+ card crashes continuously with following error:

```
SLOT X:Jul 29 09:40:52.844 UTC: %TX192-3-CPUIF_ERR: Underrun Error:
Read Pointer Crosses
Write Pointer.
-Traceback= 400310C4 411E4614 408E1934 4092B4C8 40A2FE1C 40A304F4
40110920
X=slot number
```

Conditions: Packets which have their IP header length corrupted hit the Tx E4+ card, and it causes this fatal error, causing the line card to crash.

Workaround: There is no workaround.

- CSCsk14113

Symptoms: This defect has two symptoms:

1. When changing the access lists used in LDP outbound filtering configuration **tag-switching advertise-tag for** or **mpls ldp advertise-label for**, it may result in the LSR not advertising label bindings for some prefixes.

2. If **tag-switching advertise-tags oldstyle** or **mpls ldp advertise-labels oldstyle** is configured, and the access-list used as prefix-acl in **tag-switching advertise-tags [for <prefix-acl>] [to <tsr-acl>]** or **mpls ldp advertise-labels [for <prefix-acl>] [to <lsr-acl>]** has been changed, it may result the LSR not advertise label bindings to or withdraw label bindings from peers as expected.

Conditions: Occurs in the following scenarios:

1. When changing of the access lists cause LDP performing following task:
 - Withdraw label bindings for some prefixes from a set of peers;
 - Re-advertise label bindings for these prefixes to the same set of peers;
2. The access-list explicitly permits/denies a prefix (including explicit “permit any” or “deny any”) before the change, and after the change it explicitly denies/permits a prefix (including explicit “deny any” or “permit any”).

Workaround: For problem 1:

- a. After performing the changes of access lists which cause LDP withdraw label bindings, wait for a short time to ensure label bindings have been withdrawn before performing the changes of access lists which cause LDP re-advertise label bindings.
- b. If problem already happened, recover it by performing the same changes in a pace as described in a., or toggle “mpls ip” on the interface.
- c. Change the access-list name used by prefix-acl.

For problem 2:

- a. Remove the access-list completely, with a short time to ensure label bindings have been withdrawn/advertised to all peers as expected, then add back the desired access-list.
- b. Toggling “mpls ip” on the interface.
- c. Change the access-list name used by prefix-acl.

- CSCsk15520

Symptoms: In case that multiple MPLS Traffic Engineering(MPLS-TE) Tunnels and Fast Reroute(FRR) are configured on Cisco 12000 series router, in event of FRR invoking, unaffected MPLS-TE tunnel is also protected by FRR unexpectedly.

Conditions: The MPLS-TE Tunnels are Equal Cost Multipath for BGP Nexthop. Once one of tunnels is restored by FRR, the other tunnel which is not affected may be protected also and the backup Tunnel continue “active” status in FRR database. After FRR invoking and reoptimized to a secondary path, BGP routes are balanced into both one primary tunnel and one backup tunnel which should not be activated.

Workaround: There is no workaround.

- CSCsk19661

Symptoms: In a Cisco 7500 HA router in RPR+ Mode when configuring and unconfiguring channel groups under an E1 controller, the router reports the following:

```
*Aug 22 17:58:34.970: %HA-2-IPC_ERROR: Failed to open peer port. timeout *Aug 22
17:58:34.974: %HA-3-SYNC_ERROR: CCB sync failed for slot: 1 *Aug 22 17:58:34.974:
%HA-5-SYNC_RETRY: Reloading standby and retrying sync operation (retry 1).
```

and the standby RSP is reloaded.

Conditions: This symptom is observed when configuring and unconfiguring channel groups under an E1 controller.

Workaround: There is no workaround.

- CSCsk30567

Symptoms: A GSR with Eng5 line cards may not pass traffic when acting as an ASBR in an inter-as vpn option B setup. The problem happens after the removal of a VRF from the ASBR. The mpls labels advertised on the eBGP peering for the vpnv4 prefixes are not programmed in the line cards so traffic is dropped. The label for a prefix can be seen on the RP, but not on the LCs.

Conditions: When there are lots of prefixes in BGP. Seen with PRP2 with Eng5 line cards.

Workaround: Flapping the affected prefix triggers an update which gets the labels on the LCs.

- CSCsk35283

Symptoms: Following error occurs:

```
%EE48-3-ALPHA_MCAST: Can't assign new hw_mdb
```

Conditions: Observed on E3-choc12 Line card with multicast-egress-qos enabled. At least 8 OIF for a VRF mroute on the same LC.

Workaround: Spread the VRF interface distribution so that none of the LC contain more than 7 interfaces.

Further Problem Description: Best known way to recover is through reload of the LC.

- CSCsk49685

Symptoms: In an FRR setup, VPNv4 packets are black-holed around 4-5 seconds while the traffic switched over to the backup TE-Tunnel.

Conditions: Problem is seen with Cisco IOS Release 12.0(32)SY4 for VPNv4 traffic ingress to GSR Engine-2 line card.

Workaround: There is no workaround.

Further Problem Description:

Engine-2 linecard incorrectly sets the tunnel label for tunnel-end when the traffic is forwarded to the back-up tunnel. MPLS packets arrives at the tunnel-end with 0 TTL hence they are discarded.

- CSCsk53104

Symptoms: RSP is not reused the IDB. When the maximum 2047 IDB is reached after delete and add a channel-group several times, the RSP did not assign the old IDB because is on non-share reuse mode and log the follow messages.

```
Cisco7507_test#sh idb ifnum
Interface Deleted IfIndex Feature
Se0/0/0:1 36 non-shared reuse,
Se0/0/0:1 21
Se0/0/1:3 37 non-shared reuse,
Se0/0/1:3 22
Se0/0/1:5 38 non-shared reuse,
Se0/0/1:5 23
Se0/0/1:6 39 non-shared reuse,
Se0/0/1:6 24
Se0/0/6:21 227 non-shared reuse,
Se0/0/6:21 69
Se0/0/6:21.16 70
Se0/0/6:28 600 non-shared reuse,
Se0/0/6:28 67
Se0/0/6:28.16 68
RSP logged the follow messages:
=====
Cisco7507_test(config-controller)#controller E1 6/0/6
```

```
Cisco7507_test(config-controller)#no ch 3 timeslots 4
Cisco7507_test(config-controller)# ch 3 timeslots 4
*Sep 13 14:03:15: %FIB-2-HW_IF_INDEX_ILLEGAL: Attempt to create CEF
interface for Serial6/0/6:3 with illegal index: 2049
-Traceback= 403564FC 40278C60 4027B438 402A1E3C 404ECA1C 404DEAC4
*Sep 13 14:03:16: %IPC-5-SLAVELOG: VIP-SLOT6:
Sep 13 14:03:15: %MDS-2-LC_INVALID_INPUT_IF_INDEX: Invalid input
if_index (0x801) for HWIDB allocation exceeds platform_maxinterfaces
```

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 120(32)S. This Issue happens only when reconfigure channel-groups.

Workaround: There is no workaround.

- CSCsk54203

Symptoms: When an add/drop multiplexer is in bidirectional mode, changing the APS mode using the **aps unidirectional** or **no aps unidirectional** commands, there is no APS mode mismatch message seen.

Conditions: This problem is seen on a Cisco 12416 Internet Series router containing dual Channelize OC48 line cards configured for Automatic Protection Switching. The router is booted with Cisco IOS Release 12.0(32)S6q.

Workaround: There is no workaround

- CSCsk56496

Symptoms: On router using HA RPR+, after an encapsulation change is done on serial interfaces of channelized port adapters, a reload of slave RSP is called.

Conditions: Encapsulation is changed on channelized interfaces and issue happens when you exit configuration mode.

Workaround: There is no workaround

- CSCsk61417

Symptoms: If `spa_dmlp_add_bundle(&bndl);` in `bflc_spa_dmlp_add_bundle_guts()` routine failed for first link. The flag `bundle->plim_provisioned` was set to true, making bundle unusable.

Conditions: This issue occurs when first link failed to be added to the bundle.

Workaround: There is no workaround.

- CSCsk64052

Symptoms: When an engine 3 OC48 card is reloaded, PIM neighbors over the default MDT tunnel are lost for VRFs that have interfaces configured on a linecard other than the one which was reloaded.

Conditions: VRFs configured that have interfaces defined on more than one LC might see the default MDT tunnel flap when an LC is reloaded.

Workaround: Do not reload LC.

- CSCsk70924

Symptoms: Some Frame-relay interfaces stop forwarding traffic after SPA reload.

Conditions: The issue happens with Frame-relay interfaces configured on a SPA using any of the following SIP on a Cisco 12000 series router:

- SIP-401
- SIP-501
- SIP-601

- SIP-600

Workaround: Reload the linecard with the affected interfaces.

- CSCsk72704

Symptoms: Tracebacks and spurious memory access occur when MR APS is unconfigured.

Conditions: The direction has to be changed from bidirection to unidirection before unconfiguration.

Workaround: There is no workaround.

- CSCsk75759

Symptoms: RP does not boot up if it is power cycled immediately on upgrading the ROMmon.

Conditions: Occurs only with Cisco IOS Release 12.0(33)S-based images.

Workaround: Avoid power cycle of the PRP immediately after the upgrade. Boot IOS after the ROMmon upgrade.

- CSCsk76076

Symptoms: There are no netflow data for the traffic received on the port-channel 1. There is netflow data for the traffic received on port-channel 2, but the data match with the traffic from first interface of the bundle. Netflow data are still correct for the traffic sent to a port-channel interface (netflow destination interface).

Conditions: Sampled netflow configured on GSR 12416 router, 2 port-channel configured Upgrade of the IOS from version 12.0(32).S5 to version 12.0(32).S8.

Workaround: There is no workaround.

- CSCsk84729

Symptoms: PIM neighbor will not form over tunnel interface when a VRF is re-added. If the neighbor does form, even then MCAST traffic will continue to drop on the E3 LC.

Conditions: Occurs after a VRF is removed and later on re-added. This was observed in Cisco IOS Release 12.0(32)S.

Workaround: Remove and re-add the **hw-module slot X ip multicast hw-accelerate source-table size** command. This is a traffic-impacting operation.

- CSCsk86526

Symptoms: After a long haul fiber cut is restored on DWDM equipment, the interface on E4+ is stuck.

Conditions: Occurs on the following topology:

Test GSR (E4+) ---(local fiber)--- third-party DWDM ---- long haul fiber ----- third-party DWDM
---(local fiber)--- Customer GSR

LOF is seen on E4+ which is not getting cleared upon restoration of long haul fiber cut. This is causing the interface not to come up.

Workaround: Framer is not sending an interrupt to clear the LOF in software. When LOS interrupt comes to clear LOS, check the status of LOF also and clear it if it is not present.

- CSCsk92715

Symptoms: Some Frame-relay interfaces stop forwarding traffic after SPA reload.

Conditions: The issue happens with multilink frame-relay interfaces configured on a SPA using any of the following SIP on a Cisco 12000 series router:

- SIP-401

- SIP-501
- SIP-601
- SIP-600

Workaround: Reload the linecard with the affected interfaces.

- CSCsl01899

Symptoms: The following error occurs:

```
%GSRSPA-3-UNEXPECTED_NULL_BAY error comes up when SPA is removed from linecard.  
Router# SLOt 1:00:07:09: %GSRSPA-3-UNEXPECTED_NULL_BAY: hostType 0x75, slot 1, subSlot  
0, bayCount 2 -Traceback= 4003110C 406D1668 406DBBC0 40A3AA80 40110700 SLOt  
1:00:07:09: TFIA is halted. Waiting for RP to initiate recovery
```

Conditions: This issue occurs only when a linecard has been ADMN DOWN status.

Workaround: Shut down the subslot before removing SPA.

Wide-Area Networking

- CSCsf07760

Symptoms: When many MLP sessions come up at once, the router may leak packet memory. In some cases, this may cause the router to reload.

Conditions: This symptom has been observed on Cisco 7600 and 12000 series routers. It may also occur on other models.

Workaround: There is no workaround.

- CSCsj30005

Symptoms: Changing the encapsulation on a member of a multilink bundle while the bundle is up may cause the router to reload.

Conditions: This symptom has been observed when changing an interface that is an active member of a multilink bundle from PPP to frame relay encapsulation.

Workaround: Shut down the interface before changing the encapsulation.

- CSCsk27525

Symptoms: VIP2-50 is crashing on a Cisco 7500 series router running Cisco IOS Release 12.0(31)S02y due to a DBUS error

Conditions: This problem is seen several times in a production network.

Workaround: There is no workaround.

- CSCsk58013

Symptoms: A router crashes with unexpected exception to CPUvector.

Conditions: This happens on a Cisco 7200 series router when removing CBWFQ with encapsulation frame-relay.

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.0(32)S8

Cisco IOS Release 12.0(32)S8 is a rebuild of Cisco IOS Release 12.0(32)S. The caveats listed in this section are resolved in Cisco IOS Release 12.0(32)S8 but may be open in previous Cisco IOS releases. This section describes only severity 1, severity 2, and select severity 3 caveats.

Basic System Services

- CSCee24395

Symptoms: A Cisco router may reload if SNMP GetNextObjectInstance request are processed at clogHistoryEntry_get.

Conditions: This symptom is observed on a Cisco 7206VXR series router with NPE- 300 processor board running IOS 12.2(13)T5.

Workaround: The work around is not to query the CISCO-SYSLOG-MIB. You may create a SNMP view to exclude this MIB and attach this view to all communities configured on the device. This will prevent any managers from accessing the CISCO-SYSLOG-MIB.

- CSCeg62070

Symptoms: Tracebacks or crash are seen during HTTP transactions with long URLs.

Conditions: The crash is seen when the length of any token in the URL of the request is excessively long.

Workaround: Disable HTTP server using the **no ip http server** command.

- CSCsb22489

Symptoms: In the vrf-lite configuration , the supervisor crashes when the vrfs are removed from the configuration. The crash persists even on interchanging the Wanda card and SIP-2.

Conditions: The following commad results in a Software forced reload.

```
c7606-b(config)#no ip vrf cisco3
```

OSPF was the common protocol and the crash has not been reported when bgp is configured on the router.

Workaround: This is a repeatable bug and no workarounds are known at this point.

- CSCsi77185

Symptoms: The memd recarved on RSP never occur because of the VIP stuck trying to change the MTU under Serial interface.

Before the changes:

```
=====
interface Serial5/0/1:1 mtu 2000 < ===== to be changed
ip address 10.10.10.1 255.255.255.0
no ip directed-broadcast no keepalive
```

After the changes:

```
=====
interface Serial5/0/1:1
Router(config-if)#mtu 900
RSP logged the follow messages:
===== 12:56:45:
%CBUS-3-CMD: Cmd failed: tx limit, response 0x8010, Serial5/0/1:1
-Traceback= 40349B68 404CFE38 404D5180 403C30B4 4037CF64 40390CF4 403F22C8 403F22B4
Router(config-if)#
Router(config-if)# 12:57:21:
```

```
%HA-2-IPC_ERROR: Failed to open peer port. retry queue flush 12:57:21:
%HA-3-SYNC_ERROR: CCB sync failed for slot: 1 12:57:21:
%HA-5-SYNC_RETRY: Reloading standby and retrying sync operation (retry 1). 12:57:36:
%RSP-3-SLAVECHANGE: Slave changed state from Slave to Non-participant
```

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 120(32)S. This Issue happens only on serial interfaces when you change the MTU.

Workaround: There is no workaround.

- CSCsi96900

Symptoms: A Cisco port adaptor CT3IP-50 running IOS version 12.0(32)S6 may reload unexpectedly. This has been experienced many times. The information gathered points to a software issue. This enclosure will be updated as more information is gathered.

CT3IP-50 w/ 128MB DRAM running 12.0.32.6 crashed due to:

```
%SYS-3-CPUHOG: Task ran for 123588 msec (2838/0), process = VIP Txacc loss compensation,
PC = 60308350. -Traceback= 60308358 : %SYS-2-WATCHDOG: Process aborted on watchdog
timeout, process = VIP Txacc loss compensation. -Traceback= 60030DC4 6011774C 6011C244
6010EDF4 603081D0 6030851C
```

20:32:43 UTC Mon Apr 16 2007: Breakpoint exception, CPU signal 23, PC = 0x6010CF38

Work around: Enable "no service txacc-accounting" on the RSP

Note: You may have to enter service internal first

IBM Connectivity

- CSCsf28840

A vulnerability exists in the Data-link Switching (DLSw) feature in Cisco IOS where an invalid value in a DLSw message could result in a reload of the DLSw device. Successful exploitation of this vulnerability requires that an attacker be able to establish a DLSw connection to the device.

There are workarounds available for this vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20070110-dlsw.shtml>

IP Routing Protocols

- CSCek76776

Symptoms: The issue is observed at big service provider whereas atm-sub interfaces are deleted and new one created on regular basis as they remove and add new end customers.

Because it is not a manual process as scripting is used to perform that task, old configuration from deleted sub-interface are showing up on new sub-interfaces and in some cases are creating outages.

This issue was observed in version Cisco IOS Release 12.0(27)S5d.

Workaround: verify sub-interface configuration and if configuration cannot be deleted on that sub-interface, delete this sub-interface then create a dummy sub-interface which will pull that configuration. Then recreate prior sub-interface.

- CSCin95836

The Cisco Next Hop Resolution Protocol (NHRP) feature in Cisco IOS contains a vulnerability that can result in a restart of the device or possible remote code execution.

NHRP is a primary component of the Dynamic Multipoint Virtual Private Network (DMVPN) feature.

NHRP can operate in three ways: at the link layer (Layer 2), over Generic Routing Encapsulation (GRE) and multipoint GRE (mGRE) tunnels and directly on IP (IP protocol number 54). This vulnerability affects all three methods of operation.

NHRP is not enabled by default for Cisco IOS.

This vulnerability is addressed by Cisco bug IDs CSCin95836 for non-12.2 mainline releases and CSCsi23231 for Cisco IOS Release 12.2 mainline releases.

This advisory is posted at

http://www.cisco.com/en/US/products/products_security_advisory09186a008089963b.shtml.

- CSCse07118

Symptoms: A router may reload unexpectedly when you enter the **transmit-interface** interface configuration command on an interface that has a point-to-point OSPF adjacency.

Conditions: This symptom is observed on a Cisco router when the OSPF network type is configured as point-to-point, either because the interface is, for example, a serial interface, or because the **ip ospf network point-to-point** interface configuration command is enabled on the interface.

Workaround: When there is an OSPF adjacency on the interface that is being configured, first enter the **shutdown** interface configuration command before you enter the **transmit-interface** interface configuration command.

- CSCsh53327

Symptoms: It has been observed that Cisco IOS Command Line Interface (CLI) allows user to enter multiple entries of **no ip split-horizon eigrp AS#** when the interface has not yet been assigned to a VRF interface.

Then when the interface is assigned to a VRF, these "no ip split-horizon eigrp AS#" entries stay under the interface and are not checked against the EIGRP AS number to which this interface belong.

This behavior has been observed with multiple Cisco IOS version included Cisco IOS Release 12.0(32)S5:

```
interface ATM6/0.64 point-to-point ip vrf forwarding NETWORK
ip address 10.150.10.113 255.255.255.252
no ip directed-broadcast
ip mtu 1500
no ip split-horizon eigrp 100
no ip split-horizon eigrp 1
no ip split-horizon eigrp 2
no ip split-horizon eigrp 4
no atm enable-ilmi-trap pvc 1/64
```

Workaround: before assigning an interface to a VRF, make sure no protocol configuration exist under the interface by using either the "no" statement command or the command itself to get the configuration into a default state.

- CSCsh68376

Symptoms: CBB route reflector advertising the route with different next hop, and IPFR route reflector lsanca92c14-0391 still keeps the old route in the routing table. Soft clear needed to perform on lsanca92c14-0391 to refresh the route.

Conditions: The function `bgp_suppress_ebgp_update()` does not check if the neighbor has the flag `BN_AF_NHOP_UNCHANGED`. As a result, we suppress the EBGp update incorrectly.

Workaround: clear soft in

- CSCsi03359

Symptoms: When an interface comes up, Cisco IOS triggers a PIM Hello, this hello does not always make it to the other side. The reason seems to be here that hello is sent before the port can actually forward IP packets. IGP manages to get its neighborship up but PIM not, then RPF will change to the new neighbor and in result blackholing happens up to 30 seconds.

Workaround: You could decrease the hello timer for PIM hello.

- CSCsi47635

issue observed at big service provider whereas atm-sub interfaces are deleted and new one created on regular basis as they remove and add new end customers.

Because it is not a manual process as scripting is used to perform that task, old configuration from deleted sub-interface are showing up on new sub-interfaces and in some cases are creating outages.

This issue was observed in version 12.0(27)S5d.

workaround: verify sub-interface configuration and if configuration cannot be deleted on that sub-interface, delete this sub-interface then create a dummy sub-interface which will pull that configuration. Then recreate prior sub-interface.

- CSCsi62559

Symptoms: OSPF packets with IP Precedence 0 are classified by SPD as priority packets. This is an error because only IP Precedence 6 packets should be classified as priority packets by SPD.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(18) or a later release but may also affect other releases.

Workaround: Use ACLs to block invalid IP control packets from reaching the control plane.

ISO CLNS

- CSCsg40507

Symptoms: BFD may not come up when an IP address on an interface is changed and when IS-IS is configured as the routing protocol.

Conditions: This symptom is observed only when you first enter the **router isis** command and then enter the **bfd all-interfaces** command.

Workaround: Unconfigure BFD, change the IP address, and then reconfigure BFD.

- CSCsi57971

Symptoms: IS-IS may not advertise the prefix of a passive interface to the IS-IS database on a local router.

Conditions: This symptom is observed on a Cisco router when you shut down an interface (for example, G9/1/1) of a 5-port GE SPA (SPA-5X1GE) that is installed in a SIP-600, replace the SPA-5X1GE with another card, and then enter the **no shutdown** interface configuration command on the interface at the same location (G9/1/1) on the new card. In this situation, the prefix for the interface (G9/1/1) is not advertised.

Possible Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface.

Miscellaneous

- CSCef68324

Cisco Internetwork Operating System (IOS/Æ) Software is vulnerable to a Denial of Service (DoS) and potentially an arbitrary code execution attack from a specifically crafted IPv6 packet. The packet must be sent from a local network segment. Only devices that have been explicitly configured to process IPv6 traffic are affected. Upon successful exploitation, the device may reload or be open to further exploitation.

Cisco has made free software available to address this vulnerability for all affected customers.

More details can be found in the security advisory that is posted at:

<http://www.cisco.com/warp/public/707/cisco-sa-20050729-ipv6.shtml>

- CSCek37068

Symptoms: Engine 5 Line card crashes due to IMEM SBE

Conditions: SBE in IMEM

Workaround: There is no workaround.

- CSCek42390

Symptoms: The output of "show ip mds forwarding vrf <X> <group>" command (executed on E3 Line cards) would normally show both the slowpath entries as well as the hardware switching entries. However, after upgrade to 32S2 nightly of 04/28, some of the mVRFs show only the slowpath entries for this command.

Conditions: First reported on 32S2 nightly image of 4/28. However, it could have existed before that.

Workaround: None is required. The hardware entries are still properly programmed and can be still seen using "show ip hardware-m rx vrf <X> <group>" command.

Further Problem Description: The main concerns are: - Output of the command is not consistent for different vrfs even on the same Cisco IOS image. This can lead to confusion or incorrect interpretation while troubleshooting problems. - Its not clear if the lack of hardware entries in the output of the command should be treated as normal or not. - The "expected" output of this command needs to be documented. It is suggested that this bug be used to document the 'normal'/'expected' output of the command (i.e whether hardware entries should be expected or not).

- CSCek61276

Symptoms: IPv6 traffic stops.

Conditions: This symptom is observed on a Cisco router when you first disable and then re-enable IPv6 on an interface.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface.

- CSCek69776

Symptoms: Ethernet frames with layer 2 header comprised of BEEFF00D are sent out of an MPLS TE tunnel during MPLS TE tunnel reconvergence.

Conditions: This symptom has been observed on an Engine 3 Gigabit Ethernet line card of a Cisco 12000 series router. The symptom was not present on POS line cards of the same engine.

Symptom has been observed between the time when reconvergence of all tunnels is triggered and the time when reconvergence of the particular tunnel is completed.

Workaround: There is no workaround.

- CSCek70840

Symptoms: If a multilink interface has one end connected to Cisco 12000 router and the other end connected to a non-Cisco-12000 router, then the multilink interface receiver, at the non-Cisco-12000 router side, may drop all received packets due to packet fragment loss or out-of-order.

Condition: This may happen immediately when the first member link comes back up again after all member links of the multilink interface have gone down.

Workaround: 1> Create a new multilink interface.

2> Move the member links from the current multilink interface to the new multilink interface.
- CSCek73767

Symptoms: Reload Gige SPA cause line card crash.

Conditions: Do hw-module subslot 0/0 reload then LC in slot zero crashed.

Workaround: There is no workaround.
- CSCsa92748

Symptoms: A Network Processing Engine G1 (NPE-G1) may restart unexpectedly and report the following message:

Last reset from watchdog reset

Conditions: This symptom is observed only on Cisco 7200 and Cisco 7301 series routers that are configured with an NPE-G1 Network Processing Engine.

Workaround: There is no workaround.
- CSCsd71911

Symptoms: When you make changes to an active QoS service policy, an already freed block may be accessed. If this situation occurs, a Malloc failure may occur, and the router may crash.

Conditions: This symptom is observed on a Cisco router when you make changes to an active QoS service policy while traffic is being processed.

Workaround: There is no workaround.
- CSCsd90427

Symptoms: A Cisco 7200 series router may unexpectedly reload if QOS is configured when a PA-POS-1OC3 or PA-POS-2OC3 is installed.

Conditions: This can occur on all 12.0S images prior to the fix if the device is configured with QOS and has a PA-POS-1OC3 or PA-POS-2OC3 installed.

Workaround: There is no workaround.
- CSCsd95616

Two crafted Protocol Independent Multicast (PIM) packet vulnerabilities exist in Cisco IOS software that may lead to a denial of service (DoS) condition. Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

This advisory is posted at
<http://www.cisco.com/warp/public/707/cisco-sa-20080924-multicast.shtml>.
- CSCse17960

Symptoms: A Cisco 7304 that has an NPE-G100 processor may access a bad virtual address and reload unexpectedly.

Conditions: This symptom is observed when traffic flows to an ATM VC that is configured for MLP with a QoS policy and when the QoS policy has a priority class.

Workaround: There is no workaround.

- CSCse32112

Symptoms: On an Engine 3 GE line card, after several switchovers, the **show policy-map interface** command output shows MDRR queues unallocated.

Conditions: This symptom is observed on Cisco 12000 series Internet routers with Engine3 GE line card and with 2 RPs in SSO Mode. An output service policy is applied to the line card. It happens in a systematic behavior (after the second switchover) if 8Qs/LC have been configured on the line card. It happens in a random behavior (after a random number of switchover) if 4Qs/LC have been configured on the line card (default configuration).

Workaround: There is no workaround.

- CSCse50262

Symptoms: CE to CE pings fail in an EoMPLS Network when the PE edge facing interface is newly provisioned in Port Mode (also known as the xconnect command is applied on the interface).

Conditions: This symptom is observed on Cisco IOS Release 12.0(32)SY and EoMPLS is configured in port mode, on an Engine 3 GiGE line card for a link between PE-CE, and the port is newly provisioned. This is seen only on one test bed and not seen on other test beds with the same configurations.

Workaround: The problem goes away by doing a **shut** command followed by a **no shut** command on the newly provisioned interface.

Further Problem Description: Once the workaround is applied, this problem does not happen for that port even after the router or line card reloads. It also does not affect any traffic or any customers that are added later on.

- CSCsf09508

Symptoms: When passing full 10 Gig Traffic into an E5 LC wherein the Dual priority feature is enabled and all the 10 Gig traffic is matching the higher priority criteria, the LC crashes. Conditions:

1. Dual priority feature enabled on the E5 LC
2. All the 10 Gig traffic matching the higher priority criteria.

Workaround: Don't send all 10 Gig traffic as higher priority.

- CSCsf30714

This Unexpected Reload on Cisco 12000 series routers running either GRP or PRP is seen when they are connected back-to-back and one of them is reloaded or restarted. This problem happens when BGP IPV4 prefix A recurses over a nexthop PrefixB. Also @a label is configured for the Prefix A. All works fine in normal condition but when the Nexthop router crashes or when interface connecting Prefix B flaps, the router crashes.

This problem could happen under following circumstances.

1. we have a recursive BGP route ie BGP aggregate resolved via /32 and vice- versa.
2. BGP IPv4 + label being used

Workaround: 1. Do not use BGP recursive routes.

2. Do not use IPv4 + label in the config

- CSCsg16908

Multiple vulnerabilities exist in the Cisco IOS File Transfer Protocol (FTP) Server feature. These vulnerabilities include Denial of Service, improper verification of user credentials and the ability to read or write any file in the device's filesystem, including the device's saved configuration, which may include passwords or other sensitive information.

The Cisco IOS FTP Server is an optional service that is disabled by default. Devices that are not specifically configured to enable the Cisco IOS FTP Server service are unaffected by these vulnerabilities.

This vulnerability does not apply to the Cisco IOS FTP Client feature.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20070509-iosftp.shtml>.

- CSCsg63580

Symptoms: While booting the Router the rf_db is not getting initilaized to correct values

Conditions: Normal booting

Workaround: There is no workaround.

- CSCsg78790

Symptoms: The **show policy-map interface** command output counters are not incrementing if traffic stream is muticast and Eng3 is setting qos-group on ingress.

Conditions: - Ingress policy-map classifying, and setting qos-group for received muticast traffic streams on Eng3 of c12000 node

- Egress policy-map attached to one of Eng5 interfaces, matching the qos-group set previously by Eng3 policy-map.

Workaround: There is no workaround.

- CSCsg86806

Symptoms: fast_tagrew will be missing in cef leading to imposition failure for those recursive prefixes going over a tunnel.

Conditions: recursive prefixes going over tunnel and tunnel flaps.

Workaround: clear ip route <prefix> should fix the issue.

- CSCsg90385

Symptoms: Each multicast packet has 24 bytes overhead added on both eng3 with egress qos enabled and on eng5 LC. This overhead can be seen via "sh policy-map int" counter. This is not just a counter issue, it also impacts the throughput.

Conditions: eng3 with egress qos feature enabled or eng5 lc

Workaround: There is no workaround.

- CSCsh00031

Symptoms: After router reload, the local switching traffic on the 4xgigE Eng3 LC is not restored.

Conditions: This symptom has been observed when the router reloads.

workaround: Shut down and restart the Gigabite Ethernet interfaces.

- CSCsh19361

Symptoms: OIR SFC on 12816 chassis may result in LC gets reset. The problem observed when there is L2 local switching traffic between the POS ports.

Conditions: OIR redundant SFC and there are L2 FR local switching traffic between the ports.

Workaround: There is no workaround.

- CSCsh19583

Symptoms: OIR backup CSC can result in packet loss

Conditions: Reinsert backup CSC

Workaround: There is no workaround.

- CSCsh38340

Symptoms: "show ip mds stats linecard" shows MDFS reloads on all LCs when multicast distributed routing is added on a VRF through the configuration of "ip multicast-routing vrf vpn distributed"

Workaround: There is no workaround.

Further Problem Description: Note that whilst the MDFS reload is a real reload, it is without a preceding clear so it will not generally cause traffic interruption as it merely causes the same information to be downloaded to the linecards again. However in a highly scaled system running close to the limit, the additional load introduced by a full MDFS reload of every linecard may cause additional failures owing to maxing out of the CPUs.

- CSCsh39887

Symptoms: VRF feature clean-up error messages occur When trying to delete T1 interfaces from a channel-group

Conditions: The condition occurs When trying to delete T1 interfaces from a channel-group

Workaround: Remove all the VRF configurations from the serial interface before trying to delete it.

- CSCsh41646

Symptoms: During Cisco IOS upgrade procedure on GSR, configuration from interface may be removed from running configuration.

Conditions: This issue is detected when upgrading from Cisco IOS Release 12.0(31)S2 to Cisco IOS Release 12.0(32)S2 and the missing configuration is from Gigabit Ethernet interface of SPA-1XTENGE-XFP and SIP-600 card in slot 0. Problem only appear on rare situations. Adding back configuration will restore service.

Workaround: There is no workaround.

- CSCsh52903

Symptoms: When the linecard runs into some abnormal situation, the communications between SPA and linecard may not be reliable. If it occurs, it normally triggers the SPA IPC keepalive failure. The failure of SPA keepalive/heartbeat results in SPA IPC restart. However, because of SPA IPC communications, the restarting of SPA may never be completed, leaving SPA in out of service state.

Workaround: Reloading SPA should recover the SPA.

- CSCsh55956

Symptoms: 4 Port ISE Packet Over SONET OC-12c/STM-4 line card crashes.

Conditions: feature mode is enabled and traffic is passed through it in ingress direction in PE router in a 6PE setup

Workaround: Disable feature mode using no hw-module slot <x> np mode feature.

- CSCsh59530

GSR router has been upgraded from Cisco IOS Release 12.0(31)S1C to Cisco IOS Release 12.0(32)S6. On router's reload the following error messages were printed in router's log:

```
*Jan 30 04:23:28.585 EST: %QM-4-SW_SWITCH: Interface Serial4/0/0/5:0 routed traffic
will be software switched in ingress direction(s)
```

```
*Jan 30 04:23:29.589 EST: %QM-2-TCAM_ERROR: TCAM pgm error(46): LC based QOS Mgr
failed RTR2-PE#
```

```
*Jan 30 04:23:29.589 EST: %QM-4-SW_SWITCH: Interface Serial4/0/0/10:0 routed traffic
will be software switched in ingress direction(s)
```

GSR has SIP-400 with 4CT3/DS0 SPA, with approx 30 channelized interfaces. After reload ALL channelized interfaces had both Ingress and Egress TCAM disabled.

```
RTR2-PE#sh qm int Serial4/0/0/16:0 Interface: Serial4/0/0/16:0 IP is enabled
hw[EGRESS] = 0, hw[INGRESS] = 0 hw_force_default[EGRESS] = 1,
hw_force_default[INGRESS] = 1 TCAM disabled for egress. All packets punted to LC CPU
TCAM disabled for ingress. All packets punted to LC CPU flags: message replied
```

Also spurious memory access traceback has been recorded in router's log:

```
*Jan 30 04:23:51.159 EST: %ALIGN-3-SPURIOUS: Spurious memory access made at 0x7A935C
reading 0x44
```

```
*Jan 30 04:23:51.159 EST: %ALIGN-3-TRACE:
```

```
-Traceback= 007A935C 007A8BE8 0079E1EC 007ACBE0 007AC270 002EC5CC 002F65C4 00000000
```

- **CSCsh68190**

Symptoms: After LC reset of Engine 3 CHOC48 or 4xGE or RP toggle, 'sh policy-map interface' shows subinterface attached policy to have output queues unallocated. Output also fails to show policing or WRED information.

Conditions: Engine 3 channelized OC48 on c12000 using frame-relay encapsulation on serial and POS interfaces, as well as subinterfaces configured on 4xGE card. Triggered by LC reset or RP toggle.

Workaround: Attach/re-attach policy to interface/subinterface.

- **CSCsh73935**

Symptoms: A router may reload when you perform an snmpwalk on the ciscoMvpnMrouteMdtTable.

Conditions: This symptom is observed when all of the following conditions are present:

- IP multicast routing is enabled on a VPN routing/forwarding instance (VRF)
- This VRF is associated with an interface.
- The Multicast Distribution Tree (MDT) default group address is not configured for the VRF.

Workaround: Configure the MDT default group address for the VRF by entering the **mdt default mdt group** command in VRF configuration mode.

- **CSCsh82766**

Symptoms: remove interfaces from one vrfA to another vrfB and cause mdt tunnel to flap. then remove the "mdt default" statement from vrfA, this causes LC to reset

Conditions: remove "mdt default" under obsolete configuration

Workaround: There is no workaround.

- **CSCsh90531**

Symptoms: Ping failures with MLPPP on SPA-CT3-DS0/SPA-CHOCX-DS0.

Conditions: MFR with xconnect/ATOM and MLPPP configured on the same SPA.

Workaround: Reload the SPA.

- **CSCsh91974**

Symptoms: RP crash.

Conditions: Some of the PIM CLIs are causing active RP to crash. This is happening ONLY when these CLIs are configured while in the sub-config mode for "control-plane policing". Normally, any global relevant config should automatically exit the sub-config prompt, and accept the CLI as well. In this case, the PIM command is rejected and RP crash follows. The same PIM commands work fine when executed under the global config mode (where they belong) or under other sub-config modes.

Workaround: Use the "exit" command to exit the the main config prompt before configuring PIM related CLIs.

- CSCsh96294

Symptoms: OSPFv3 neighbor down may occur after upgrading IOS to 12.0(32)S release.

Conditions: IOS 12.0(32)S release is used.

Workaround: There is no workaround.

- CSCsi01470

A vulnerability in the Cisco implementation of Multicast Virtual Private Network (MVPN) is subject to exploitation that can allow a malicious user to create extra multicast states on the core routers or receive multicast traffic from other Multiprotocol Label Switching (MPLS) based Virtual Private Networks (VPN) by sending specially crafted messages.

Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080326-mvpn.shtml>.

- CSCsi11485

Symptoms: A Cisco 12000 router running 12.0(32)SY2b image exhibits large number of memory usage on the RP and reduce in its Largest Free Block (fragmentation) compare to earlier release of 12.0(32)SY1.

This is seen on E0 ATM, E3 ATM, and E3 GE and is suspected to be impacting other types of engines and line cards as well.

Conditions: This appears to be impacting line cards with larger number of IDBs (subinterfaces.)

Workaround: There is no workaround.

- CSCsi12586

Symptoms: When ALPHA has an error due to some bug, the linecard crashes without error recovery.

Workaround: There is no workaround.

Further Problem Description: During any ALPHA errors, there is no trace of the problem occurring. This happens only during SW bugs, but should be fixed to improve debuggability.

- CSCsi13242

Symptoms: Destination interface value showing wrongly in netflow cache.

Conditions: problem can be seen on c12kprp-p-mz.120-nightly.S for engine4+ card.

Workaround: This problem is not seen on engine3 and engine5 cards .

- CSCsi13685

Symptoms: 4-port E3 GE LC stuck in UP state for about 45 minutes before coming to RUN state.

Conditions: This issue was seen in scaled IP+L3VPN+mVPN environment when the router was reloaded.

Workaround: Reloading the LC resolves the issue.

- CSCsi18200

Symptoms: The following error message is logged:

```
%LC_MOD48-3-SPAG_MULTIPLE_BAY_EFC_BP_MAPPED_TO_CONGA_PORT: Found EFC channels from 2 different bays mapped to the same Conga port. existing map {bay=1, efc_chn=238}, requested map {bay=2, efc_chn=238}
```

Conditions: This error message while reloading SPAs that has multilink bundle (Multilink FR or Multilink PPP) configuration. This issue is specific to the SPA interfaces on SIP-400.

Workaround: There is no workaround.

- CSCsi40941

Symptoms: The use of time-based WRED on an output service policy results in different min-max threshold values on E3 and on E5 for identical policy.

Conditions: Policy configured that is using time-based WRED.

Workaround: conf t hw-module slot <E5-slot#> qos use-e3-std-for-wred

- CSCsi52321

Symptoms: After inserting a 4OC48E/POS-SR-SC LC it is recognized but when command "upgrade mbus-agent-rom" is used LC is not recognized by the router anymore and displays:

```
%MBUS-6-OIR: 4 Port ES Packet Over SONET OC-48c/STM-16 Removed from Slot x MBus agent ROM upgrade failed on slot x (rc=5)
```

Conditions: New LC is inserted in the chassis and have never been upgraded its ROM code before.

Workaround: There is no workaround.

- CSCsi58063

Symptoms: RP crashes when CSC is shut down by command.

Conditions: This symptom has been observed when CSC is shut down.

Workaround: There is no workaround.

- CSCsi63432

Symptoms: Tracebacks on microcode reloading SIP-400.

Conditions: Service policy attached on MFR subinterfaces and microcode reload done

Workaround: There is no workaround.

- CSCsi63889

Symptoms: SIP always reload by itself when our link were down for one site

Conditions: This issue happens when a NF is configured.

Workaround: Disable NF.

- CSCsi64245

Symptoms: C12000 dual RP with Engine 5 line card traceback SEC 0:00:01:48:

```
%EERP-3-INVALID_UIDB_HWIDB_MAP: slot 7, index= 00000004 orig_if= GigabitEthernet7/0/0 given_if= GigabitEthernet7/0/0 free= 0
```

```
-Traceback= 212BF8 212D00 82027C 81BDFC 81B0B4 12EEE4 181908 181B04 1826A0 125F6C 1990B4 199434 192BC8 192E2C 193128 193DD0
```

Conditions: C12000 Engine 5 interface configuration change when system has dual RP

Workaround: There is no workaround.

- CSCsi67310
Symptoms: After RP switchover, all configured WRED thresholds are set to 0 in "sh policy-map int" command
Conditions: 1. After RP switchover
2. Only on eng5 MPLS trunk
3. Only when the output policy is an unnested policy-map
Workaround: Remove service-policy from the interface and re-attach it or shut/no shut the interface
- CSCsi69492
Symptoms: EoMPLS traffic stops on E4+ on CSC switchover
Conditions: Execute CSC switchover by shutting primary CSC. EoMPLS traffic forwarding stops.
Workaround: To recover, execute mic-reload of E4+ line card.
- CSCsi78221
Symptoms: Engine 3 stuck over minutes (found to be 20 minutes)
Conditions: During BMA recovery
Workaround: There is no workaround.
Further Problem Description: Card resets.
- CSCsi81511
Symptoms: Fails to drain the half packets during error recovery
Conditions: When error recovery is triggered and traffic passes into the Mod48 , during error recovery , it fails to drain the half packets and fails to initialise the congs.
Workaround: There is no workaround.
- CSCsi96067
Symptoms: Process memory leaks on FRoMPLS router
Condition: - configuring "service-policy output" on the interface, - flowing traffic heavy enough to be policed by the configuration.
Workaround: There is no workaround at this moment.
Further Problem Description: Flowing about 110 pps traffic, the router crashes with %SYS-6-STACKLOW on the FR LMI process.
- CSCsj04991
Symptoms: QoS on egress port of E4+ POS is not taking effect if the tunnel headpoint on the same port as well.
Conditions: The issue happens when we remove the "mpls ip" configuration under the tunnel and re-add it after a delay.
This does two things.
1.This corrupts and resets the feature processing flag in the ingress adjacency which normally enables "feature processing in the egress". Since this is reset to 0, the egress is not able to do QoS.
2. The adjacency rewrite info corresponding to the tunnel in the egress gets removed.
Workaround: Remove "mpls ip" from the tunnel interface once and immediately add it back. This corrects the issue.

- CSCsj05541

Symptoms: 'show interface' command indicate that egress data rate on 4GE-SFP-LC shows doubled rate of actual traffic rate.

Conditions: EoMPLS setting on the interface may cause this issue. It can be seen with PRP-2 and GRP-B.

Workaround: There is no workaround.
- CSCsj06177

Symptoms: RPR+ mode, when I do the following sequence the slave RSP configs add a "shutdown" command under interface serial.

Conditions: RSP runnig RPR+

Workaround: Doing the follow steps interface serial x/x shut no shut
- CSCsj08112

Symptoms: On a GSR running Cisco IOS Release 12.0(32)S6o all non ipc tofab queues are depleted on a choc12/ds1-ir-sc line card causing all traffic to be dropped including Layer 2 control traffic for the interfaces.

Conditions: This condition was seen again three days after the first occurence.

Workaround: There is no workaround.
- CSCsj09009

Symptoms: Local Switching -- like to like and Interworking is not working on E3 gig LC.

Conditions: Local Switching -- like to like and Interworking is not working on E3 gig LC. Traffic starts and stops forwarding after some time.

Trigger: Doing shut/noshut on the core facing port of the same LC

Workaround: There is no workaround.
- CSCsj09104

Symptoms: Line protocol of E3 QOC12 goes down on mic-reload.

Conditions: mic-reloading the line card.

Workaround: There is no workaround.
- CSCsj09740

Symptoms: SPA-2XOC48POS/RPR goes to Out Of Service after encountering a SPA BUS ERROR. TRANSCEIVER-6-REMOVED messages were followed by SCC failure resulting the SPA to go to Out Of Service.

Conditions: Lots of L1 errors are found (B2-BER) on the link and the interfaces flapped lot of times before the BUS ERROR.

Workaround: LC reload.
- CSCsj09792

The channelized OC12 controller on a GSR might go down and remain down in case of a PLIM CPU reset. If this occurs, APS may not switch to the other channel.

"show aps" will display that the active channel's interface is down: router#sho aps CHOCx 3/0 APS Group 3: protect channel 0 (Active -interface down)

Workaround: There is no workaround.

Recovery: In case of a PLIM cpu reset, if the controller stays in the down state, the line card must be reloaded with the "test mbus <slot> power off/on" commands.

- CSCsj14388

Symptoms: BFD session goes down on removing and adding ip address from bfd enabled interface.

Conditions: This symptom is observed on a GSR router loaded with Cisco IOS Release 12.0(32)SY image. After BFD sessions are established on adding and removing ip address couple of times the BFD sessions go down

Workaround: Reload the routers.

- CSCsj15162

Symptoms: The following error message occurs on CHOC12/DS1-IR-SC linecard indicating that the PLIM is reset:

%LC_CX3-2-PLIM_RESET: PID 49165, CAUSE 0

Conditions: When shutdown / no shutdown was executed on many multilink ppp bundles continuously.

Workaround: There is no workaround.

- CSCsj25144

Some CEF related commands on a previously removed sub interface are (wrongly) retained when configuring a new sub-interface. This is also true for sub-interfaces that are being reused.

Symptoms: The following CEF related commands are retained from previously removed sub-interfaces:

- ip cef accounting non-recursive external - ip load-sharing per-packet

For example:

```
Router(config-if)#int Serial3/3/1:0.100 point <<< ADD .100
Router(config-subif)#ip cef accounting non-recursive external
Router(config-subif)#ip load-sharing per-packet
Router(config-subif)#no int Serial3/3/1:0.100 <<< REMOVE
Router(config)#int Serial3/3/1:0.200 point <<< ADD .200
Router(config-subif)#do sh run int Serial3/3/1:0.200 Building configuration...
Current configuration : 166 bytes ! interface Serial3/3/1:0.200 point-to-point
no ip directed-broadcast ip load-sharing per-packet <<<<
ip cef accounting non-recursive external <<<<
no ip mroute-cache end
```

Conditions: This issue is observed in 12.0S on reused and new ATM or serial sub-interface on a GSR.

Workaround: Verify sub-interface configuration and if configuration cannot be deleted on that sub-interface, delete this sub-interface then create a dummy sub-interface which will pull that configuration. Then recreate the prior sub-interface.

The problem is not seen in 12.2S branches and later.

- CSCsj28901

Symptoms: When changing mtu on 4xOC3-V2 SPA in SIP-501, the following crash may be seen: %RP-3-CARVE_FAIL: FrFab BMA, slot 9 %RP-3-COREDUMP: Core dump incident on slot 9, error: Safe FrFab buffer carve failure %RP-4-RSTSLOT: Resetting the card in the slot: 9,Event: linecard error report %LCINFO-3-CRASH: Line card in slot 9 crashed

Conditions: This symptom is observed on a Cisco 12000 series router that runs the c12kprp-p-mz image of Cisco IOS pre-Release 12.0(32)SY4.

Workaround: There is no workaround.

- CSCsj28914

Symptoms: SPA may reset due to heartbeat failures on doing CSC switchover. Following messages may be seen. SLOT 4:1d19h: %SPA_PLIM-3-HEARTBEAT: Subslot 3 has experienced an heartbeat failure Current Sequence 31064 received Sequence 31057 Time since last keep 1000ms.

Conditions: SPAs in SIP-401/501/601 Doing CSC switchover.

Workaround: There is no workaround.

- CSCsj29012

Symptoms: On rommon upgrade of secondary RP after an IOS upgrade, the active RP may crash

Conditions: Dual RP set up. IOS upgrade done by reloading the secondary RP followed by redundancy force switch over. When the router is up, perform rommon upgrade on secondary RP.

Workaround: There is no workaround.

- CSCsj30638

Symptoms: On doing OIR of CSC cards or during Cisco IOS upgrades, the CSC card may be recognised as SFC or vice versa. In case of non-redundant fabric configuration, the linecards may go into low bandwidth mode. This may result in configs being lost.

Conditions: Seen during Cisco IOS upgrades to 32SY or during OIR of CSC cards

Workaround: Reload the router to come out of the situation

- CSCsj34705

Symptoms: When upgrading from 120-28.S4c to 120-32.S6p some tcam carve configuration commands are lost for an engine 3 card.

Conditions: Examples of some of the tcam recarve commands are:

```
hw-module slot 4 tcam carve RX_TOP_NF 3
hw-module slot 4 tcam carve RX_144b 35
hw-module slot 4 tcam carve RX_288b 45
hw-module slot 14 tcam carve RX_TOP_NF 3
hw-module slot 14 tcam carve RX_144b 35
hw-module slot 14 tcam carve RX_288b 45
```

These commands may fail to show up in the configuration after an upgrade.

Workaround: Reconfigure commands and microcode reload linecard.

- CSCsj35153

Symptoms: SLOT 3:Jun 19 17:17:17.632 EDT:

```
%DATACORRUPTION-*1*-%DATAINCONSISTENCY: copy error -Traceback= 4003111C
40045CCC 4005F3A0 409CA48C 409CC660
```

Conditions: Just after upgrading one c12000 from 28S4c to 32S6p, while doing the upgrade all all, the following tracebacks were observed in the log.

Workaround: This is a non-intrusive trace. There is no need for a workaround or operator intervention.

- CSCsj36294

Symptoms: Router crash and crash dumped to bootflash

Conditions: While loading grp image labelled for 06/16 for 32s image.

Workaround: There is no workaround.

- CSCsj38190

Symptoms: After RPR+ switchover, native multicast traffic may get dropped on Engine 5 linecards

On the egress linecard do: **sh ip mds for***affected s g* and retrieve the hw_mdb **sh controller multicast mgid-table** *hw_mdb* should return something like: table_value[0]:200043AFFFFFFF table_value[1]:0 The table_value[0] should END In FFFFFFFF when this problem occurs

Conditions: Only affects E5 It has only been seen on the 32s release (32.S6o, 32.s6p]

Workaround: Any of the following will work: flap the affected interface clear the mroute [**clear ip mroute** * reload mdfs [**clear ip mds line** *linecard num*]

- CSCsj44020

Symptoms: When engine 3 4xGE linecard cpu is busy, packets may be forwarded to the wrong interface on the linecard when multiple configuration events are happening.

Conditions: Multiple configuration events, for example removing multiple output service policies on an interface or subinterface level.

Workaround: Configure fewer multiple configuration events.

- CSCsj45048

Symptoms: pw adjacency is created on the RP.

Conditions: Any.

Workaround: There is no workaround.

Further Problem Description: Backing out this fix will cause MLPPP bundle unprovisioning with a traceback "%RP-3-ENCAP:Failure to get output encapsulation:unprovisioning MLPPP mem"

- CSCsj47840

Symptoms: Output NF not working on 32S8 16/06 dated coded image for Engine5 card

Conditions Configure Output NF on Engine-5 card and check for NF cache

Workaround: There is no workaround.

- CSCsj50949

Symptoms: MVPN Decap node classifying multicast traffic stream according to the GRE tunnel IP Precedence. show policy interface packets counter incrementing for the wrong class/queue.

Conditions: - P node (GSR), with ingress E3 line card. Ingress MQC policy re-marking (set ip precedence) multicast traffic. - C12000 act as MVPN Decap node, ingress E3 line card with egress multicast policy enabled. Traffic matching P re-marked IP Precedence.

Workaround: No workaround.

- CSCsj60303

Symptoms: SIP401 crashes.

Conditions: Stressing the LC with the following set of events :

- 1) Multilink3 and Multilink8 with 2 members each
- 2) Flap one of the members of multilink3 by changing crc
- 3) Shut down the members of multilink3
- 4) Removed the members of multilink3 and chaged the encap to default encap
- 5) Delete multilink3
- 6) Add multilink3 back
- 7) Add the members back to multilink3
- 8) Flap the link of multilink8 by changing the crc

This is applicable to both MLPPP as well as MFR Bundles.

Workaround: There is no workaround.

- CSCsj93643

Symptoms: In rare cases, C12000 router with SIP400 and one or more SPA-CT3/DS0 and SPA-T3E3 installed may display the following message:

```
SLOT 14:Jul 22 06:18:31.790 EDT: %SPA_PLIM-3-HEARTBEAT: Subslot 2 has experienced an
heart beat failure Current Sequence 1980 received Sequence 1970 Time since last keep
2952ms.
```

SPA-CT3/DS0 and SPA-T3E3 may stay in the state and the SPA may not recover in some cases.

Workaround: The following command may be used to disable SPA heartbeat to avoid the SPA failure.

```
execute-on <slot#> test hw-module subslot <subslot#> ipc keepalive disable
```

It is not recommended to use this command and it may lead SPA stuck in bad state. The test command shall be used under Cisco Support supervision.

- CSCsk13647

Symptoms: E5 SIP-601 LC CPU stays almost at 100% for a very long time, the WAHOO MCAST DELE process utilizing most of the CPU.

Conditions: This is seen after the MSE router reload on the scale testbed with scaled IP, L3VPN and mVPN configs.

Workaround: There is no workaround.

Wide-Area Networking

- CSCsh44649

Symptoms: Standby router may crash in SSO mode.

Conditions: mutlink interface is removed and partner router is reloaded.

Workaround: Use RPR-PLUS mode.

- CSCsi10322

Symptoms: The interface level commands 'no ppp link reset' and 'no ppp lcp fast-start' disappear from the configuration after performing a 'wr mem' or 'show run | inc ppp'. The commands do not reappear after reload.

Conditions: Interface level configuration of 'no ppp lcp fast-start' and 'no ppp link reset'

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.0(32)S7

Cisco IOS Release 12.0(32)S7 is a rebuild of Cisco IOS Release 12.0(32)S. The caveats listed in this section are resolved in Cisco IOS Release 12.0(32)S7 but may be open in previous Cisco IOS releases. This section describes only severity 1, severity 2, and select severity 3 caveats.

Basic System Services

- CSCsh63542

Symptoms: The following SNMP error message and tracebacks are seen:

```
SEC 8:000049: Jan 31 22:25:00.760: %SNMP-3-DVR_DUP_REGN_ERR: Attempt for dupe
regn with SNMP by driver having ifIndex 709 and ifDescr Tunnel0
-Traceback= 204128 204230 92DB90 92DF6C B2CF8C BBF368 BC00C8 1C4EFC 1C5524
1C60B8 1C655C 2EC5CC
```

Conditions: This symptom has been observed when new interfaces are added (or existing interfaces like tunnel come up) after bootup, or when new or existing interfaces come up after RPR+ switchover when running Cisco IOS Release 12.0(32)S6. Also, this symptom occurs if the **snmp ifindex persist** command is configured on the router.

Workaround: There is no workaround.

Further Problem Description: Though customer traffic is not affected, this symptom does impact the SNMP stats and other SNMP data for both the original and the new interface. Usually the message is from the standby RP, so once that standby RP becomes active, the data from SNMP polls of these interfaces would not be accurate.

Interfaces and Bridging

- CSCds44777

Symptoms: The data terminal ready (DTR) port adapter on a Cisco router does not continuously drop and pulse according to the time intervals configured with the **pulse-time seconds** interface configuration command. On the 4-port serial port adapter (PA-4T+) and Fast Serial Interface Processor (FSIP), the iRSP-3-RESTART message may appear right before a Cisco router has to be restarted to recover a serial interface from a circuit outage that was configured by entering the **pulse-time seconds** interface configuration command.

Conditions: This symptom is observed on a Cisco 7500 series router that a PA-4T+ port adapter, an 8-port serial port adapter (PA-8T), and an FSIP.

Workaround: There is no workaround.

IP Routing Protocols

- CSCdu59038

Symptoms: A Cisco router or switch may reload unexpectedly when you enter the **show ip eigrp neighbors EXEC** command.

Conditions: This symptom is platform independent and is observed when you enter the **show ip eigrp neighbors EXEC** command immediately after you have entered the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command for the interface that connects the router or switch to the neighbor.

Workaround: Wait for the neighbor list to be completely rebuilt before you enter the **show ip eigrp neighbors EXEC** command.

- CSCdu73495

Symptoms: Enhanced Interior Gateway Routing Protocol (EIGRP) routes cannot be seen even when message digest algorithm 5 (MD5) is authenticated on all routers. This symptom is intermittent and may occur when authentication is turned off and subsequently turned back on again. Sometimes, this symptom occurs just after authentication is enabled.

Conditions: This symptom has been observed when authentication is turned off and subsequently turned back on again and sometimes just after authentication is enabled.

Workaround: This symptom is intermittent and may be resolved by disabling and reenabling authentication a second time. This symptom may automatically be resolved after a few minutes.

- CSCdx83729

Symptoms: A summarized entry may remain in the Enhanced Interior Gateway Routing Protocol (EIGRP) topology table after manual summarization is disabled.

Conditions: This symptom is observed when manual summarization is enabled and subsequently disabled on a network that is also being redistributed into EIGRP.

Workaround: Restart the EIGRP process.

- CSCed84633

Symptoms: The *interface-type* and *interface-number* arguments in the **distribute-list** address family configuration command do not function.

Conditions: This symptom is observed on a Cisco platform that integrates the fix for caveat CSCea59206. A list of the affected releases can be found at

<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCea59206>. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

Workaround: There is no workaround.

Further Problem Description: The fix for CSCed84633 re-enables the *interface-type* and *interface-number* arguments in the **distribute-list** address family configuration command for both VRF interfaces and non-VRF interfaces.

- CSCsg55209

Symptoms: When BGP updates are received, stale paths are not removed from the BGP table, causing the number of paths for a prefix to increase. When the number of BGP paths reaches the upper limit of 255 paths, the router resets.

Conditions: This symptom is observed on a Cisco router when the **neighbor soft-reconfiguration inbound** command is enabled for each BGP peer.

Workaround: Remove the **neighbor soft-reconfiguration inbound** command. A router that runs a Cisco IOS software image that has a route refresh capability, storing BGP updates is usually not necessary.

ISO CLNS

- CSCse40346

Symptoms: Tracebacks may be generated when you configure IS-IS and LDP features, for example, when you enter the **no ip router isis area-tag** command.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(32)SY but may also occur in other releases.

Workaround: There is no workaround.

Miscellaneous

- CSCee63182

Symptoms: A Cisco 7200 series or another mid-range router may crash or may stop responding.

Conditions: This symptom is observed on a Cisco 7200 series or other mid-range router that runs Cisco IOS Release 12.3(6a). The crash occurs when an interface that is configured with a **rate-limit** command is deleted by entering the **no interface** command and then reenabled by entering the **interface** command.

Workaround: Remove the rate-limit configuration from the interface before deleting the interface.

- CSCek59056

Symptoms: Engine 4+card netflow drop 5%+ flows.

Conditions: This symptom is observed on Cisco IOS Release 12.0(26)S with GSR Eng4+ LC sampled netflow.

Workaround: There is no workaround.

- CSCek70165

Symptoms: A CEF inconsistency can occur after a switchover in RPR+ mode.

Condition: This issue has been seen on a Cisco 12416 Cisco Internet Series router containing dual PRP-2 Route Processors running Cisco IOS Release 12.0(32)S6. The route contains 11 Engine 3 and 3 Engine 4+ line cards. The CEF inconsistency has been seen on both Engine 3 and Engine 4+ line cards.

Workaround: There is no workaround.

- CSCek71514

Symptoms: A master timer may be accessed prior to being initialized. This can be seen by the following error message:

```
SEC 7:000048: Nov 30 00:00:29 GMT: %SYS-3-MGDTIMER: Uninitialized timer, init with
uninitialized master, timer = 53E62C0. -Process= "Init", ipl= 0, pid= 3
```

Condition: This symptom is seen on a Cisco 12416 Cisco Internet Series Router containing dual PRP-2 processors running in RPR+ mode. This router is booted with Cisco IOS version 12.0(32)S6.

Workaround: There is no workaround.

- CSCsd18278

Symptoms: In a rare condition, the line card CPU may be hogged and fails to process SPA IPC messages. The back-pressure of SPA interface may cause SPA interface card overflow with its IPC internal FIFO and make SPA interfaces down.

Conditions: This symptom has been observed on an SPA interface.

Workaround: There is no workaround.

- CSCsd73139

Symptoms: The crashinfo is returning the message "device or resource ready".

Conditions: If the LC gets reset before the crashinfo file is closed, the open bit is set

Workaround: There is no workaround.

- CSCsd92818

Symptoms: The SIP-400 LC crashes and recovers when the CE2 is reloaded. The CE is a Cisco 7200 with PA-8TE1's connecting via a Mux to the GSR. The CT3 SPA on the GSR has quite a few MLP & MLFR interfaces for VPN services using biscuit. MVPN is also turned on for these VPNs.

Conditions: This symptom has been observed on a GSR with SIP-400 w/4xCT3 SPA.

Workaround: There is no workaround. The LC crashes and recovers.

- CSCse11720

Symptoms: On a GSR running Cisco IOS Release 12.0(31)S, the BFD session is dropped after lost of One BFD control packet.

The actual BFD interval is constantly higher than the interval configured, in the traces below the tx interval is configured to 2s and the actual Tx interval is around 3,5s

Conditions: This is a BFD-enabled BGP session between two GSR, x.x.x.1 with a tx timer of 5s, and x.x.x.x.2 with a tx timer of 2s. Both multiplier are 3. Both routers are running Cisco IOS Release 12.0(31)S, and both sides are Engine 3 linecards.

This is a sniffer trace.

```
#30: BFD control packet A from .2 to .1
#31: BFD control packet A from .2 to .1 (3,575848s after #30)
#33: BFD control packet A from .2 to .1 (3,511843s after #31)
#34: BFD control packet A from .2 to .1 (3,623851s after #33)
#36: BFD control packet A from .2 to .1 (3,167859s after #34)
#37: BFD control packet A from .2 to .1 (3,655841s after #36)
#38: BFD control packet A from .2 to .1 (3,359866s after #37)
#42: BFD control packet A from .2 to .1 (3,255843s after #38)
#44: BFD control packet A from .2 to .1 (3,471862s after #42)
#46: BFD control packet A from .2 to .1 (3,639842s after #44)
#47: BFD control packet A from .2 to .1 (3,287859s after #46)
```

After the lost of one BFD control packet, the BDF session is down.

```
#48: .1 signals the session down 6.003069 s after having received #47
```

```
6.003069 s is the detection time 3 x 2 s (our mult x .1's tx timer)
```

Workaround: There is no workaround.

- CSCse29728

Symptoms: When setup ATM to ATM local switch over a l2tpv3 tunnel, the PE router might reload at atm_l2trans_vc_get_segment_handle_fr_ac_ie_hdl

Conditions: The ATM setup is VPTrunk with cellrelay, and this symptom has only observed on Cisco 7500 platform as PE router in the topology.

Workaround: There is no workaround.

- CSCse67197

Symptoms: On removal of a member from portchannel VRF interface, router crashes.

Conditions: This symptom has been observed on removal of a member from portchannel VRF interface.

Workaround: There is no workaround.

- CSCsf99866

Symptoms: Sending mpls traffic to an E5 LC with oc-192 SPA which doesn't have mpls configured, it will cause this LC crash.

Conditions: This symptom has been observed with an E5 LC with oc-192 SPA. This symptom does not happen if using 10G SPA or E4+ oc-192.

Workaround: There is no workaround.

- CSCsg05390

Symptoms: The following message is unexpectedly seen on an E4+ LC:

```
%TX192-3-PAM_MODULE:
```

Conditions: No conditions have been identified so far. This section is being completed as more information is available.

Workaround: There is no workaround.

Further Problem Description: This is the complete log that is seen on the router:

```
SLOT 12:Aug 11 07:51:39: %TX192-3-PAM_MODULE: status = 0x2, mask= 0x3F -
MODULE: Error signal from PIM module.
-Traceback= 40030CBC 40862008 408625EC 4096046C 40960B08 4010F8C8
SLOT 12:Aug 11 07:51:39: %TX192-3-PAM_PIM: status = 0x3D6, mask= 0x181 - PIM:
header start offset >= 16kB.
-Traceback= 40030CBC 408621A4 40862634 4096046C 40960B08 4010F8C8
SLOT 12:Aug 11 07:51:39: %GSR-3-INTPROC: Process Traceback= 4011717C 40110290
40011180
-Traceback= 40030CBC 4075AB8C 40960D60 4010F8C8
SLOT 12:Aug 11 07:51:44: %GSR-3-INTPROC: Process Traceback= 400F9B34 40117140
-Traceback= 40030CBC 4075AB8C 40960D60 4010F8C8
Aug 11 07:51:49: %LDP-5-NBRCHG: TDP Neighbor 10.10.10:0 is DOWN (TCP
connection closed by peer)
Aug 11 07:51:57: %LDP-5-NBRCHG: TDP Neighbor 10.10.10.72:0 is UP
SLOT 12:Aug 11 07:52:28: %TX192-3-PAM_MODULE: status = 0x2, mask= 0x3F -
MODULE: Error signal from PIM module.
-Traceback= 40030CBC 40862008 408625EC 4096046C 40960B08 4010F8C8
SLOT 12:Aug 11 07:52:28: %TX192-3-PAM_PIM: status = 0x356, mask= 0x181 - PIM:
header pkt length >= 16kB.
-Traceback= 40030CBC 408621A4 40862634 4096046C 40960B08 4010F8C8
SLOT 12:Aug 11 07:52:28: %GSR-3-INTPROC: Process Traceback= 409AFC9C 40117178
-Traceback= 40030CBC 4075AB8C 40960D60 4010F8C8
SLOT 12:Aug 11 07:52:33: %GSR-3-INTPROC: Process Traceback= 409AFC9C 40117178
-Traceback= 40030CBC 4075AB8C 40960D60 4010F8C8
```

- CSCsg26943

Symptoms: After perform a RP switchover on a long idle(20 hrs above) GSR router loaded with 092806 nightly build image, all LCs got reset.

Conditions: This symptom has been observed when all LCs are reset, after RP switchover on a long idle router.

Workaround: There is no workaround.

- CSCsg37491

Symptoms: IPv4/IPv6 ping failed over L2TPv3 Tunnel. This is happening with PD also and here IPv6 ping fails.

Conditions: 1) Create a L2TPv3 tunnel .. establish a Ipv6/ipv4 adj. b/w the CE's 2) Send a Ipv4/ Ipv6 traffic. 3) Do a reload/SSO of the router ... you should hit this issue.

Workaround: E3 Gig. LC reload on decapsulating router solves the symptom.

- CSCsg50381

This issue is not related to TE/FRR specific. Issue in driver code handling read/write to hardware. Linecard is crashing because we are writing to hardware without stopping the pipeline. TE/FRR config has exposed this issue because TE/FRR updates happen in interrupt mode.

- CSCsg77355

Symptoms: LC may crash at multicast code area after deprovision and reprovision mlp interface that has pim enabled

Workaround: There is no workaround.

- CSCsg77370

Symptoms: After deprovision and re-provision MLP interface and its associated serial link interfaces several times, error msg may appear. After this error msg, you can no longer define the same mlp interface.

```
%ERP-2-UIDB_ERR: Unable to allocate resources. Invalid slot for free -1
```


Conditions: De-provision & re-provision MLP interface several times.

Workaround: There is no workaround.

- CSCsg99698

Symptoms: After adding and deleting MLPPP interface, RP switchover and then change the encapsulation to FR interface, error msg %IDBINDEX_SYNC-3-IDBINDEX_ENTRY_SET can occur and standby RP can crash.

Workaround: There is no workaround.

- CSCsh17373

Symptoms: SIP 601 resting when netflow is unconfigured.

Conditions: This symptom is seen with c12kprp-p-mz.120-32.S5.1213 build.

Workaround: There is no workaround.

- CSCsh23048

Symptoms: Spurious memory access at tfib_check_attached_parent

Conditions: Recursive prefix going over attached parent and parent is load shared. That is, there is multiple path to reach parent prefix. And, there is no tag information for attached or connected parent prefix. When recursive child prefix is resolved, it will access NULL tag_info and tag_rewrite of connected/attached parent prefix and result in spurious access.

Workaround: In vrf address family, give the command “redistribute connected” and/or “redistribute static”. Also, configure static route instead of static recursive route by specifying interface option in the static route configuration, if any exist. LFIB does not effectively support static recursive route configuration.

- CSCsh23370

Symptoms: ATM port mode, after adding xconnect statement under ATM interface, the interface continues flapping until shut/noshut the interface

Conditions: This symptom has been observed when provisioning xconnect statement under ATM interface.

Workaround: Shut/no shut the interface.

- CSCsh31719

Symptoms: Mod48 LC crashes continuously with IPC messages from SPA.

Conditions: In customer network having MLPPP links CT3 SPA and Serial interfaces on CT3 and T3 SPAs with VRFs configured and having large no of BGP routes.

Workaround: There is no workaround.

Further Problem Description: The symptom happening because of corrupted IPC packet coming from SPA. As part of solution Sanity checks and buffer corruption correction code added to avoid crashes. More details in the attached log mail.

- CSCsh35160

Symptoms: During the OIR of SPA, the following syslog messages may appear and soon after the E5+ SIP 601 LC will reload.

```
SLOT 2:*Jan 5 18:50:13.984 UTC: %EE192-3-SPABRG_DRV: wwolf_handle_spa_removed: too
many spas for grp: 0x0, 0x0, 0x0
-Traceback= 40A2751C 405E1ED0 405C437C 405CDBC0 40657C94 4074A360 406D0F64 406D2104
4121901C 406D0798 406D2374 406CFC98 406CFF00
```

```
SLOT 2:*Jan 5 18:50:34.732 UTC: %EE192-3-SPABRG_DRV: wwolf_spa_init: queue group not
found: 0x0, 0x0, 0x0
-Traceback= 40A2751C 405E1A78 405CD0AC 40657C74 4074956C 406D1A8C 4121901C 406D0798
406D2374 406CFC98 406CFF00
```

Conditions: This symptom can occur on rare occasions of OIR of SPA's on E5+ SIP 601 LC.

Workaround: After each OIR of spa wait at least 2 minutes and then insert any new spa.

- CSCsh42982

Symptoms: A Cisco 12410 with SIP-405/501/601 linecard with 5x1GE SPA and BFD configured and operating in RPR-Plus redundancy mode, break BFD sessions when redundancy force failover is initiated.

Conditions: Redundancy mode must be RPR-Plus BFD must be configured Force failover must be initiated

Workaround: Admin shut down the interface, wait for 15 seconds and then 'no shutdown' the interface to recover the BFD session.

- CSCsh44224

Symptoms: When sending 10 Gig traffic to a 2.5 Gig interface, the egress data rate as seen in the 2.5 gig pos spa interface is 9.4 G/s which is higher than the supported bandwidth.

Conditions: This symptom has been observed on a 2.5 Gig POS SPA interface.

Workaround: Correctly configure the network to avoid this scenario.

- CSCsh46154

Symptoms: On SIP-600, we are seeing the error message to be logged on the console as below.

```
SPA error interrupts are not yet
```

Conditions: This symptom has been observed on a SIP-600.

Workaround: Reset the SIP-600 card.

- CSCsh46431

Symptoms: After issuing "hw-module slot x reload", the pseudowire vc stays down since there is no local label allocated

Conditions: This symptom has been observed after a line card reload.

Workaround: Removed and then add the **xconnect** command. Shutting down and restarting the interface does not work.

- CSCsh55026

Symptoms: After RPR+ forced switchover, traffic is no longer passed across the affected frame-relay subinterfaces on the CT3 SPA. Commands ran on SPA LC indicate the incorrect mapping of if_number.

Conditions: RPR+ switchover must occur, BGP needs to be running, and routes injected, we hit it with 180,000 routes.

Workaround: Workaround is to reload the slot which the CT3 SPA is in.

- CSCsh56006

Symptoms: Ce-ce ping/traffic fails, mip reg counter increments on remote pe condition: Frompls, with both PE's reload simultaneously workaround: need to unprovision both atom vc;s on both Pe's, unprovisioning on one Pe doesn't work.

Workaround: There is no workaround.

- CSCsh58550

Symptoms: A PXF crash could happen if multiple combinations of features are present: input ACL, input QoS, output ACL, output QoS.

Conditions: The crash will happen only if the input policymap is first disabled on the input interface ('no service-policy input X') and then it is de-configured on the router ('no policymap X').

Workaround: There is no workaround.

- CSCsh67166

Symptoms: The packets might get punted to Tx slow-path. FRR switchover will not happen in 50ms time.

Conditions: This symptom has been observed when primary link goes down and backup tunnel takes over.

Workaround: There is no workaround.

- CSCsh75078

Symptoms: RP failover would cause SIP-601 core-facing line card to crash, and reload.

```
%RP-4-RSTSLOT: Resetting the card in the slot: 15,Event:linecard error report
%LINK-5-CHANGED: Interface GigabitEthernet15/0/0, changed state to
administratively down
%OSPF-5-ADJCHG: Process 2, Nbr 10.0.0.45 on GigabitEthernet15/0/0 from FULL to
DOWN, Neighbor Down: Interface down or detached
%LDP-5-NBRCHG: LDP Neighbor 10.0.0.45:0 (1) is DOWN (Interface not operational)
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet15/0/0, changed
state to down
%PIM-5-NBRCHG: neighbor 10.144.2.13 DOWN on interface GigabitEthernet15/0/0 non DR
%LCINFO-3-CRASH: Line card in slot 15 crashed
%MBUS_SYS-3-NOBUFFER: Message from slot 15 in stream 1 dropped
%MBUSFLASH-3-TIMEOUT: No response from slot 8 (type 5,time 2000)
%BGP-5-ADJCHANGE: neighbor 172.16.1.2 vpn vrf m1 Up
%BGP-5-ADJCHANGE: neighbor 172.16.2.2 vpn vrf m1 Up
%RP-3-EXEC_SLOT: Slot 15 not enabled
```

Conditions: This symptom has been observed on a Cisco 12000 node fully populated with E3 line cards, mvpn configuration, and large scale multicast routes and traffic.

Workaround: There is no workaround.

- CSCsh79487

Symptoms: Eng3 LC card crashes.

Conditions: This symptom has been observed when the LC received the 255.255.255.255 broadcast packets.

Workaround: There is no workaround.

- CSCsh81465

Symptoms: Output interface counters are incorrect.

Conditions: Traffic Generator -- G7/0/0 (SIP-600) GSR (SIP-601) G8/0/0 -- CRS-1(1) -- CRS-1(2)-- Same Traffic Generator

When generating 9.5Gbps of traffic the interface counters of Cisco 12000 populated with SIP-601 and SPA-1XTENGE-XFP showed the 5 minute output rate to be ~ 6.23 Gbps. CRS-1 interface connected to SIP-601 shows 5 minute input rate to be ~ 9.4 Gbps.

Workaround: There is no workaround.

- CSCsh89375

Symptoms: When a multilink bundle has one end connected to Cisco 12000 router and the other end connected to a non-Cisco-12000 router, the multilink interface receiver, at the non-Cisco-12000 router side, may drop all received packets due to packet fragment loss or out-of-order.

Conditions: This may happen when the first member link of the multilink bundle comes up immediately after all member links of bundle have gone down.

Workaround: There are two possible workarounds.

1. Try this workaround first.
 - a. Shut down all member links of the multilink bundle using the **shutdown** command.
 - b. Wait for 1 minute.
 - c. Bring up the member link interfaces one-by-one using the **no shutdown** command.
2. If the above workaround (option 1) does not resolve the symptom, perform the following steps:
 - a. Shut down all the links in the affected multilink bundle using the **shutdown** command.
 - b. Remove all the links from the bundle using the **no multilink-group** command until the bundle has no link.
 - c. After a few minutes (~5 min) add the links back to the same bundle using the **multilink-group group number** command.
 - d. Perform the **no shutdown** command on all the links.

- CSCsh89437

Symptoms: If cleanup is not done on CIs used by L2TPV3, and these CIs are reused by other applications, then it will have extremely undesirable effects (like in case of MLP on SIP 400/2 or 4 Port CT3/DS0 SPA, all packets get dropped). To avoid this L2TPv3 codebase has to clean up explicitly.

Conditions: Configure L2TPv3. Configure MLP. Shutdown the L2TPv3 tunnel and then shutdown the MLP. Then do a no shut on the MLP bundle. If the MLP reuses, the CI used by L2TPv3, then packets will get dropped.

Workaround: There is no workaround.

- CSCsh98714

Symptoms: Memory leak while running MLFR provisioning test script.

Conditions: Test script used for provision/reprovision an MLFR bundle including associated member links appears to trigger a memory leak on the route processor (PRP-2).

Workaround: There is no workaround.

- CSCsi07088

Symptoms: Customer has a 12000-SIP-601 that crashes and leaves no crashinfo file.

Conditions: This occurs if MBE (and SBE) parity errors occur in the SIP-601 memory.

Workaround: Repeated instances would yet point to a defective hardware.

- CSCsi16489

Symptoms: When E4P/E6 drops MTU exceeded packets coming in with aggregate label in mpls vpn setup

Conditions: In MPLS VPN environment, when the core side interface of disposition router is E4P/E6 and QOS is configured on the interface then all packets received with aggregate label that are punted to RX CPU for processing (for example MTU exceed packets) are dropped by the cef switching code.

Workaround: Change the configuration to avoid aggregate labels.

- CSCsi16530

Symptoms: BFD is not supported on Bundle interface. When user tries to configure BFD on link bundle, the router crashes.

Conditions: This symptom has been observed when applying BFD configuration on Pos-channel and ether-channel.

Workaround: There is no workaround.

- CSCsi21733

Symptoms: SPA-2XOC48POS/RPR goes to Out Of Service after encountering a SPA BUS ERROR. TRANSCEIVER-6-REMOVED messages were followed by SCC failure resulting the SPA to go to Out Of Service.

Conditions: Lots of L1 errors are found (B2-BER) on the link and the interfaces flapped lot of times before the BUS ERROR.

Workaround: Reload the line card.

- CSCsi25309

Symptoms: Packets from E5 to E2 get dropped on E2. On E2, the **show contr events** command shows the counters for "Tx short encap entry" increase.

Conditions: This symptom has been observed when Output ACL is configured on E2.

Workaround: Remove output ACL on E2.

Resolved Caveats—Cisco IOS Release 12.0(32)S6

Cisco IOS Release 12.0(32)S6 is a rebuild of Cisco IOS Release 12.0(32)S. The caveats listed in this section are resolved in Cisco IOS Release 12.0(32)S6 but may be open in previous Cisco IOS releases. This section describes only severity 1, severity 2, and select severity 3 caveats.

Basic System Services

- CSCse08044

Symptoms: A Cisco router may generate export packets in which the first flow record contains incorrect data such as incorrect IP addresses.

Conditions: This symptom has been observed on a Cisco router that is configured for NetFlow and NetFlow Data Export.

Workaround: Disable NetFlow.

- CSCse10074

Symptoms: The active RP may crash when traps are sent to a host to which an SNMPv3 user is assigned.

Conditions: This symptom is observed only when an SNMPv3 user is configured with security level noAuthNoPriv or authPriv, when the same SNMPv3 user is assigned to the host through the **snmp-server host** command, and when this command includes the **priv** keyword. This is an improper configuration.

For example, the symptom occurs when traps are triggered after the following software configurations has been applied:

```
snmp-server user TESTUSER TESTUSER v3
snmp-server group TESTUSER v3 priv notify *tv.FFFFFFFFF.FFFFFFFFF.FFFFFFFFF.F
snmp-server host 10.1.1.10 version 3 priv TESTUSER
snmp-server enable traps
```

Workaround: Do not create an improper configuration.

- CSCse29653

Symptoms: The following may be seen when attempting to boot a Cisco 12000 router that has a GRP-B RP:

```
Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x502B96C8
-----
```

```
Possible software fault. Upon recurrence, please collect
crashinfo, "show tech" and contact Cisco Technical Support.
-----
```

```
-Traceback= 502B96C8 50770F54
$0 : 00000000, AT : 55230000, v0 : 00000000, v1 : 0B0D0B0D
a0 : 0000000A, a1 : 5775A568, a2 : 00000003, a3 : 58374B58
t0 : 00000048, t1 : 58D9FE04, t2 : 58D9FE00, t3 : 58D9FDFC
t4 : 58D9FDF8, t5 : 58D9FDF4, t6 : 58D9FDF0, t7 : 58D9FDEC
s0 : 58374860, s1 : 58374864, s2 : 58374864, s3 : 58374860
s4 : 55A20000, s5 : 00000000, s6 : 00000000, s7 : 00000000
t8 : 0D0D0D0D, t9 : 00000000, k0 : 30408400, k1 : 30410000
gp : 5522BCE0, sp : 58374828, s8 : 00000000, ra : 502B9694
EPC : 502B96C8, ErrorEPC : F6BF7BFF, SREG : 3400BF03
MDLO : 3B5BF4D5, MDHI : D253FCD7, BadVaddr : 0B0D0B35
Cause 00000010 (Code 0x4): Address Error (load or instruction fetch) exception
```

Conditions: This symptom is observed on a Cisco 12000 series router that runs the gsr-p-mz image of Cisco IOS Release 12.0(32)SY.

Workaround: Attempt to boot again.

- CSCsh14643

Symptoms: VIPs do not boot up on a Cisco 7500 router.

Conditions: This symptom has been observed with a normal boot up.

Workaround: There is no workaround.

Further Problem Description: RSP emits DBUS-3-SW_NOTRDY and CBUS-3-CCBPTIMEOUT messages for all VIPs and VIPs do not boot up.

Interfaces and Bridging

- CSCeg55131

Symptoms: Spurious memory access occurs when removing channel groups in the T1/E1 cards.

Conditions: This symptom has been observed with a PA-MC-8TE1+ port adapter on a Cisco 7500 router running Cisco IOS Release 12.0S.

Workaround: There is no workaround.

IP Routing Protocols

- CSCei29944

Symptoms: A CE router that has L2TP tunnels in an MPLS VPN environment with about 1000 VRFs may crash and generate the following error message:

Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x50766038

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(32)S and that functions as a CE router when BGP neighbors are unconfigured via the **no neighbor ip-address** command while the **show ip bgp summary** command is entered from the Aux console. The symptom is not release-specific and may also affect other releases.

Workaround: There is no workaround.

- CSCsd15749

Symptoms: Prefixes that are tagged with Site of Origin (SoO) values may not be filtered at the border.

Conditions: This symptom has been observed when SoO values are configured for a peer group. The peer group members may not correctly filter the prefixes that are based on the SoO value at the border.

Workaround: BGP supports Dynamic Update peer groups, which ensure that packing is as efficient as possible for all neighbors regardless of whether or not they are peer-group members.

Peer groups simplify configurations, but peer-templates provide a much more flexible solution to simplify the configuration than peer groups.

If the SoO configuration is applied directly to the neighbor or to a template, the symptom does not occur. Using templates to simplify the configuration is a better solution and Dynamic Update peer groups ensure efficiency.

- CSCse68877

Symptoms: A label mismatch may occur between the CEF table and the BGP table, and a new label may not be installed into the CEF table.

Conditions: This symptom has been observed after a BGP flap has occurred on a Cisco router that is configured for MPLS VPN but that does not function in an inter-autonomous system and that does not have multiple VRFs.

Workaround: There is no workaround. After the symptom has occurred, enter the **clear ip route** command for the affected VRF.

- CSCsf99057

Symptoms: OSPF stub-router advertisement feature doesn't work with RPR+ and SSO when RP switchover took place. After RPR+/SSO switchover took place, the newly active RP never advertise max-metric router LSA.

However, if NSF doesn't configured on the switch, it is desirable to advertise max-metric router LSA.

Conditions: The system condition affected by this problem is below.

- The router which has dual RP and configured with RPR+ or SSO(non-NSF).
- Redundant RP is in "Standby-Hot" state.
- The **max-metric router-lsa** command is configured for OSPF in router configuration mode.

Workaround: If RP redundancy mode is configured as RPR, then OSPF stub-router advertisement feature work correctly.

- CSCsg37116

Symptoms: After giving the command **traceroute ip** *x.x.x.x* or **traceroute** *x.x.x.x* over an LDP-enabled network, the penultimate hop router shows a traceback message in the console log.

Conditions: This symptom has been observed when the mpls ip option is configured in the network and for the core trunks.

Workaround: The issue seems to be avoided if you instead enter the **traceroute mpls ipv4 A.B.C.D/32** command.

- CSCsg59699

Symptoms: The OSPFv3 cost on PortChannel interfaces calculated based on the interface bandwidth may not be correct if the **auto-cost reference-bandwidth** command is used under the ipv6 ospf router mode..

Conditions: This symptom has been observed when the auto-cost reference-bandwidth command is used under the ipv6 ospf router mode.

Workaround: Use the **shutdown** command followed by the **no shutdown** command on the PortChannel interface.

Miscellaneous

- CSCed83616

Symptoms: A Cisco router may reload when you enter the **show standby** or **show standby brief** command.

Conditions: This symptom has been observed on a Cisco router when multiple HSRP groups are configured and unconfigured in a loop while traffic for the HSRP groups is being processed.

Note, however, that a stress scenario in which many HSRP groups are configured and unconfigured while the **show standby** or **show standby brief** command is being entered may be a rather uncommon scenario.

Workaround: Do not enter the **show standby** or **show standby brief** command while configuration changes are being made.

- CSCeg74772

Symptoms: When you enter the **clear cef linecard** command, IDBs may be hold on the line card. When you enter the **clear cef linecard** command, the number of IDBs that are used on the line card increases.

Conditions: This symptom has been observed on a Cisco platform when a GRE tunnel interface is used.

Workaround: There is no workaround.

Further Problem Description: When many tunnel interfaces are used and when the **clear cef linecard** command is entered several times, the SWIDB number may reach its upper limit. If this situation occurs, you must reload the platform.

- CSCek57494

Symptoms: All packets may be dropped across a T1 or E1 link on which class-based shaping is configured.

Conditions: This symptom has been observed on a Cisco 7200 series that has an NPE-G1 and that runs Cisco IOS Release 12.2(28)SB.

Workaround: There is no workaround.

- CSCek61974

Symptoms: Cisco IOS router supporting BFD (Bi-Directional Forwarding Detection) will be able to configure minimum receive interval as low as 1 ms.

Conditions: If BFD minimum receive interval is configured below 50 ms, it can cause undesirable effects on the router. Also minimum receive interval below 50 ms is not supported in Cisco IOS.

Workaround: Configure minimum receive interval of 50 ms or higher in Cisco IOS.

- CSCek62546

Symptoms: Dual RP GSR reached an unreachable state during maintenance window, while new interfaces were being commissioned.

Once in this state, most of the interfaces on the router were down/down, and could not be brought up by shutting down and restarting or by reloading the line card.

Conditions: The memory leak was found in a function call made by the **write memory** command when NTP is running and/or the **clock calendar-valid** command has been configured.

Workaround: The router was reloaded to recover from this state. (RP switchover was also found to recover the router).

Further Problem Description: For these instances, the **show controller csar queues** command showed that the Free Queue available are 0, and all F/Q have been allocated and not released.

- CSCsc25844

Symptoms: The standby RSP crashes in loop just after config sync by TLB exception

Conditions: This symptom has been observed on a Cisco 7500 with dual RSP4+ running Cisco IOS Release 12.0(31)S2 and configured for SSO.

Workaround: There is no workaround.

- CSCsc31082

Symptoms: When performing the **show policy-map interface MFR** command, the counters do not increment.

The counters in **show policy-map interface MFR** do not increment for any type/class of service. Even the class-default shows 0 packets. The counters in **show frame-relay pvc** show the packets correctly.

Conditions: This symptom has been observed when a map-class is configured under an MFR (FRF.16) bundle (sub- interface). This map-class consists of both an input and output service-policy.

Workaround: There is no workaround.

- CSCsd55004

Symptoms: A FRR backup tunnel undergoes reoptimization, resulting in the teardown of the old lsp that is carrying traffic for primary lsps that have cutover to the backup tunnel.

Conditions: This symptom has been observed with:

- TE tunnel protecting interfaces/links.
- Usual triggers for re-optimization (link up, timer expiry, etc).

Workaround: There is no workaround.

- CSCsd60816

Symptoms: A customer running a Cisco 12000 series router with a Cisco 12000-SIP-400 and SPA-4XCT3/DS0 and SPA-4XT3/E3.

Conditions: This symptom has been observed when a CE connected to the SPA-4XCT3/DS0 via a Multilink Frame Relay interface if the interface is shut down. When the interface is restarted, interfaces on the SPA-4XT3/E3 flap.

Workaround: There is no workaround.

- CSCsd71119

Symptoms: ATM PVCs that are configured for OAM may go down because OAM cells are not properly received on the ATM PVCs. When this situation occurs, the ATM interface remains in the up/up state, but the subinterfaces on which the PVCs are configured enter the down/down state. Subinterfaces on which PVCs are configured without OAM remain in the up/up state, but traffic does not pass.

Conditions: These symptoms are observed on a Cisco Catalyst 6500 series switch that runs Cisco IOS Release 12.2SXF. However, the symptom is platform- and release-independent.

Workaround: Reset the affected interface or reload the line card on which the affected interface is configured.

- CSCsd91557

Symptoms: For local switching MFR configuration, on a GSR with a CT3 SPA, packets greater than 1500 bytes are not being forwarded.

Conditions: This symptom is observed on hardware-based E5 engine line cards on a Cisco IOS Release 12000 series that is configured for Local switching

Workaround: There is no workaround.

- CSCsd92448

Symptoms: Standby keeps crashing in SSO mode on the Cisco 7500 platform.

Conditions: This symptom is observed when dMPLP+QoS+IPHC is configured on a Cisco 7500 series router and tries to bring up the standby.

Workaround: There is no workaround.

- CSCsd98928

Symptoms: A router may crash when you enter the **show policy-map interface** command while an automated script completes the policy map and then removes the policy map during cleanup.

Conditions: This symptom is observed on a Cisco router when you enter the **show policy-map interface** command while, at the same time, the automated script removes the policy map.

Workaround: There is no workaround.

- CSCse47898

Symptoms: The line card of a Cisco 12000 series router reloads without creating a crashinfo file. %LCINFO-6-ZERO_BYTE_CI_FILE error may be reported.

Conditions: This symptom happens when all of the following conditions are met:

- Cisco 12000 Series router runs Cisco IOS software.
- Line card that is crashing is POS.
- Line card reloads when it receives from the network an MPLS packet with explicit NULL label.

Workaround: Reconfigure explicit null (**mpls ldp explicit- null**) from all routers in the VRF.

Further Problem Description: Explicit NULL label advertising is disabled by default in Cisco IOS.

- CSCse48018

Symptoms: Interface counters are double counted for tag-tag switching. This is seen on Cisco 12000 series router.

Conditions: This symptom has been observed with Engine3 card.

Workaround: There is no workaround.

- CSCse69837

Symptoms: A Cisco 12000 router with an 8OC03/ATM/TS-IR-B 8-port OC-3 ATM Line card will reload (or require a manual reload) after the line card console is flooded with %QM-4_STUCK and %PM622-2-SAR_POLL_TIMEOUT.

Conditions: This symptom has been observed when LSP paths change or when the core link flaps in the network.

Workaround: Do a soft reload of the line card.

- CSCse84226

Symptoms: When a VC is down, the output of the **show connection** command on the local side shows that the VC is up, even though the output of the **show mpls l2 vc detail** command shows that the VC is down. The output of the **show connection** command on the remote side shows that the VC is down.

Conditions: This symptom is observed on a Cisco router that is configured for AToM when the MTU mismatches the Virtual Private Wire Service (VPWS) circuit.

Workaround: There is no workaround.

- CSCse98594

Symptoms: Engine 3 4 x 1 GigE line card stops receiving any traffic. All the packets ingressing on the Gigabit interface are counted as overruns (rfifo_full).

Conditions: This symptom has been observed under following scenarios:

1) Misconfiguration in switched network caused broadcast storm to be flooded into the Gig port and the port entered into stuck state and did not forward any traffic. All other ports on the same LC were working fine.

2) In a lab scenario, the problem could be reproduced with line rate bidirectional traffic of small sized packets (64 bytes or less) with some ARP packets prevented the Gig port for receiving any further traffic with rfifo_full incrementing.

Workaround: Reloading the line card restores traffic on the Gig port

Further Problem description: This issue can be identified with following commands.

1. Check for increments in the following counters GigabitEthernet 0 denotes port "0" in the LC
LC-Slot3#show controllers Gigabitethernet 0 mac | inc frmLstIntRcvMacErr
frmLstIntRcvMacErr: 0x22B92568CF

LC-Slot3#show controllers Gigabitethernet 0 mac | inc rfifo_full 0 risl, 0 riq, 0 rdrop, 0 rsupp,
0 rinvalid_encap, 149148306788 rfifo_full
2. The RX queue pointers does not change while executing the below command repeatedly for few times

LC-Slot3#show controllers Gigabitethernet 0 fpga bm queues

- CSCsf03576

Symptoms: After router reload, error msg continues coming out on console.

Conditions: This symptom has been observed in SSO mode, not RPR+.

%TAGCON-3-LCLTAG_ALLOC: Cannot allocate local tag

Workaround: There is no workaround.

- CSCsf28763

Symptoms: Router crashes and moves to rommon mode

Conditions: This symptom has been observed with crompls configs with mpls- TE.

Workaround: There is no workaround.

- CSCsf96095

Symptoms: When customer uses one MPLS-TE tunnel for EoMPLS traffic and add and bring up new tunnel which does not use for traffic, unexpected traffic drop happened on EoMPLS.

Condition: This symptom has been observed when both TE-tunnel destinations are the same. Traffic drop happens at first tunnel up after changing pseudowire-class. No problem at subsequent flap.

Workaround: There is no workaround.

- CSCsf96559

Symptoms: MBUS ram agent fails to allow IDEEPROM on some cards to be updated - written from IOS, IDS (Manufacturing Diags) and likely IOX as well. Some or all attempts to write to the IDEEPROM will FAIL. This Affects Field Diagnostics, OBFL (Blackbox) , and any functions within IOS that update the IDEEPROM. The list of affected cards appears below.

Conditions: This symptom has been observed when running field diagnostics against any of the following products, The testing may complete successfully (or with errors, properly detecting faulty hardware) and then the Field Diags ceases to complete writing eeprom results back to CSC (or a ny fab card tested).

```
f-diag5#diag 16 prev
  Field Diag eeprom values: run 2 fail mode 0 (PASS) slot 16
    last test failed was 0, error code 0

f-diag5#diag 16 verbose
Running DIAG config check
Redundancy available: testing permissable, 5 active xbars
Executing Field Diagnostics on fabric cards may cause momentary loss
of traffic through fabric once testing has completed
Verbose mode: Test progress and errors will be displayed
Running Diags will halt ALL activity on the requested slot.[confirm]
f-diag5#
PID of f_diag_run is 192, set test_pid[16]
gdb slot is 0
Launching a Field Diagnostic for slot 16
Removing fabric card 16 from active config
Done removing UUT card from fab
Test: 1 Iris Registers
FDIAG_STAT_PASS, test 1 Iris Registers
Test: 2 Register Test
FDIAG_STAT_PASS, test 2 Register Test
Test: 3 Fabric FPGA Registers
FDIAG_STAT_PASS, test 3 Fabric FPGA Registers
Test: 4 XCVR Loopback
00:07:30: %MBUS-6-FABCONFIG: Switch Cards 0x1E (bitmask)
Primary Clock is CSC_1
Fabric Clock is Non Redundant
Bandwidth Mode : 40Gbps Bandwidth
FDIAG_STAT_PASS, test 4 XCVR Loopback
FINAL STATUS, PASS
Field Diagnostic ****PASSED**** for slot 16
```

```
Field Diag results from eeprom before updating slot 16, run# 0x2 were 0x0
previous field diag eeprom values: run 2 fail mode 0 (PASS)
last test failed was 0, error code 0
```

Now, notice run# not updated:

```
f-diag5#diag 16 prev
Field Diag eeprom values: run 2 fail mode 0 (PASS) slot 16
last test failed was 0, error code 0
```

Then further, the card will not allow a re-test.

```
f-diag5#diag 16 verbose
Sorry... Field diagnostics already running on requested board
```

The following cards are likely affected:

73-10474-01	PCA, MBRD, PSC-1, GSR
73-8812-10	PCA, SUB, PRP2, GSR
73-9615-01	PCA, SUB, CSC160-OSP, GSR
73-9718-02	PCA, SUB, ENHANCED CSC160, GSR12810
73-9719-01	PCA, SUB, ENHANCED CSC256, GSR12816
73-9870-03	PCA, SUB, PRP1, GSR
73-9617-01	PCA, SUB, SFC256-OSP, GSR
73-9618-01	PCA, SUB, CSC256-OSP, GSR

This symptom was found as a result of testing for other DDTS related to Field Diags and EEprom results and related bugs.

Workaround: There is no workaround. An MBUS Agent upgrade is needed.

- CSCsf99087

Symptoms: In using E5 interface as a CE facing interface, when the ce facing interface is enabled for SNF on output direction, the line card stops forwarding traffic after close to 16k packets have been punted to CPU for SNF.

Conditions: This symptom has been observed when using an E5 interface as a CE facing interface.

Workaround: Remove the SNF configuration from the CE facing interfaces in output direction.

- CSCsg03826

Symptoms: An OC48E/POS-SR-SC-B linecard is experiencing high CPU and soft drops after a Cisco IOS upgrade from Cisco IOS Release 12.0(31)S2 to Cisco IOS Release 12.0(32)SY. This is causing latency in traffic.

Conditions: This symptom has been observed with a

Workaround: There is no workaround.

- CSCsg17957

Symptoms: A router may crash when forwarding an IP fragment.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(28)SB3 and that is configured for L2TP and QoS.

Workaround: Remove the QoS configuration. If this is not an option, there is no workaround.

- CSCsg18982

Symptoms: A policy-map with one class that matches on an extended ACL - used for rate-limiting pings in this case - cannot be applied to an interface on a SIP-600 nor a SIP-601. The following error message is displayed: "SLOT 0:Oct 2 12:49:34.502 EDT: %EE48-5-TM_PROC: Add Profile Mgr failure for intf Serial0/0/3.451: 1" This error message is followed by a traceback.

Conditions: This symptom has been observed when trying to apply the policy-map to an interface on the SIP-600 and SIP-601.

Workaround: Use the **rate-limit** command at the interface level in conjunction with an ACL to perform rate-limiting.

Further Problem Description: The service-policy will show up in the configuration; however, it does not function.

- CSCsg22369

Symptoms: In a MPLS TE Fast Reroute environment, if a protected link were to be flapped ('down' followed by 'up'), all primary LSPs protected by a backup tunnel and going over the link, would undergo reoptimization (replacement of old FRR Active LSP with new LSP). For 0 bw primary TE tunnels (such as primary auto-tunnels), the new LSP ends up being protected by a suitable NHOP/NNHOP backup tunnel, but when the backup tunnel goes down later for some reason, the new primary LSP isn't re-evaluated and moved off the backup tunnel.

Conditions: This symptom has been observed when:

- A PLR (MPLS TE FRR Point of Local Repair) is running Cisco IOS Release 12.0S or Cisco IOS Release 12.2S.
- 0 bw fast-reroutable primary TE tunnel(s) is traversing the PLR.
- Flap of the protected link.
- An event that requires the LSP for the backup tunnel protecting the primary's TE LSP, to be torn down.

Workaround: There is no workaround.

- CSCsg22767

Symptoms: Packet counter is wrong for policy map on control plane.

Conditions: This symptom has been observed when applying policy on control plane of 2 LC of same router.

Workaround: There is no workaround.

- CSCsg26237

Symptoms: On ISE ATM LC, after vbr-nrt SCR rate is changed. The PVC needs to be bounced before the traffic gets policed by the new SCR rate.

Conditions: This symptom has been observed when vbr-nrt SCR is changed. Only police function is not working. All traffic in other class queues would use new SCR rate automatically.

Workaround: bounce PVC

- CSCsg26943

Symptoms: After perform a RP switchover on a long idle(20 hrs above) GSR router loaded with 092806 nightly build image, all LCs got reset.

Conditions: This symptom has been observed when all line cards get reset, after RP switchover on a long idle router.

Workaround: There is no workaround.

- CSCsg31554

Symptoms: SNMP ifIndex does not exist for MFR subinterfaces on CHOC12/DS1-IR-SC ISE line card after removal and reinsertion (OIR) of the card.

Conditions: This symptom has been observed in Cisco IOS Release 12.0(32)SY1 when using a configuration with a large number of serial interfaces configured, including a 8xDS1 MFR bundle. The MFR interface had a corresponding point-to-point subinterface with one DLCI defined. The subinterface was pollable before removal and insertion of the card, but the ifIndex is missing afterward.

Workaround: By reloading the router, or removing the subinterface and readding it, the ifIndex will be recreated.

- CSCsg32015

Symptoms: Port mode EoMPLS, after CE gigE interface is bounced, the PE Eng3 gigE interface does not stay up and keep on flapping until you bounce the PE gigE interface as well. This problem does not happen when VLAN is configured.

- CSCsg36725

Symptoms: A memory leak and memory exhaustion may occur when QoS policies are updated on 40,000 sessions.

Conditions: This symptom is observed on a Cisco 10000 series but may also affect other platforms.

Workaround: There is no workaround.

- CSCsg37485

Symptoms: After removing and re-applying a policy-map with hierarchical class-based policer on a Vlan sub-interface on an Engine5/SIP-601 line card, all policer counters displayed in **show policy-map interface** are zero despite traffic being sent through the interface, and the policer no longer drops excess traffic when configured to do so.

This symptom could also affect other SIP-601 interfaces/SPA's and other ingress QoS configurations.

Condition: This symptom has been observed under the following conditions:

1. There is a hierarchical shaper configured in the outbound direction on the main interface (L3/nC/mD ISE QoS model).
2. Netflow is enabled on the main interface.

Workaround: There is no workaround other than avoiding the above conditions. A line card reload temporarily fixes the problem, but once the configuration is toggled again, the symptom resurfaces.

- CSCsg40032

Symptoms: Perform a line card reload on an Engine 0 CT3 or DS3 line card, upon recovery any frame-relay sub-interfaces on those line cards which have rate-limit output configured will no longer have this applied.

Conditions: This symptom has been observed when performing a line card reload.

Workaround: Reload of the router or a reload of the ingress line card resolves the issue.

- CSCsg40339

Symptoms: MPLS OAM pings and trace from tunnel head to tail fail.

Conditions: MPLS pings and traceroutes are sent from tunnel headend to tail. They were seen failing at penultimate hop when the router had E4+ ingress line card and E5 egress line card. When E4+ is used both as ingress and egress line card, issue is not seen.

Workaround: There is no workaround.

- CSCsg42604

Symptoms: OC48 interface on 2xOC48 SPA starts flapping and does not recover.

Conditions: 2xOC48 SPA and 2x1GE SPA are co-resident in same SIP601 LC. GE interfaces are configured for EoMPLS Pseudowires. To verify CSCek30312, the **negotiation auto** command was configured on GE interface. The GE interfaces start flapping. OC48 interfaces also start flapping. With **no negotiation auto** command, GE interfaces stop flapping but OC48 keeps flapping. GE interfaces do not resume forwarding traffic.

Workaround: There is no workaround.

- CSCsg45798

Symptoms: After OIR of the SPA-4XCT3/DS0 SPA, some of the frame-relay sub-interfaces no longer forward traffic.

Conditions: This symptom has been observed when an online removal and insertion is done on the SPA-4XCT3/DS0 SPA.

Workaround: Perform a shut/no shut on the sub-interface to correct the issue.

- CSCsg46888

Symptoms: Ethernet frames with layer 2 header comprised of BEEFF00D are sent out of an MPLS TE tunnel during MPLS TE tunnel reconvergence.

Conditions: This symptom has been observed on Engine 3 gigabit ethernet line card of a Cisco 12000 series router. Problem was not present on POS line cards of the same Engine.

Symptom is observed between the time when reconvergence of all tunnels is triggered and the time when reconvergence of the particular tunnel is completed.

Workaround: There is no workaround.

- CSCsg51661

Symptoms: An E2 line card crashes.

Conditions: This symptom has been observed while applying Hw-module ip load-sharing per-packet.

Workaround: There is no workaround.

- CSCsg53254

Symptoms: On Cisco 12816/E5 running Cisco IOS Release 12.0(32)S5, packets are lost after activating the standby CSC or a SFC.

Conditions: After shutting down and then activating the standby CSC or a SFC (ex hw-module slot 16 shut / no hw-module slot 16 shut" there is traffic lost .

Workaround: There is no workaround.

- CSCsg60084

Symptoms: In a Cisco 7500 router, when we attach a Service policy to a MFR bundle that has the Serial Interface - member links configured for vip based fair-queueing, the VIP having the Serial Interfaces will crash.

Conditions: The crash is seen when attaching the Service Policy to a MFR bundle with traffic flowing the same.

Workaround: Disable the fair-queue command in the serial interfaces before adding them as member links to the MFR bundle.

- CSCsg64068

Symptoms: For both 1xchoc12-ds1 and 4xchoc12-ds3, deleting the channel informations under Sonet controller, the definitions are removed on the primary RP but not the standby RP.

Conditions: This symptom has been observed when running SSO mode only.

Workaround: Reload standby RP.

- CSCsg66019

Symptoms: After an RPR+ switchover traffic ingress on a SIP-600 and egress on 4xGE ISE LC or 10xGE E4+ LC was being forwarded on the wrong VLAN.

Conditions: This symptom has been observed when an RPR+ switchover occurs.

Workaround: There is no workaround.

- CSCsg71033

Symptoms: On a Cisco 12816 running Cisco IOS Release 12.0(32)S5, the E6 card continues to be crashed to IPC timeout when deactivating the standby CSC and activating the CSC. The same problem occurs when deactivating a SFC and activating the SFC.

E6 card continues to be crashed to IPC timeout which was caused by continuously incremental CRC errors in FIA from output of the **show controller fia** command until the whole Cisco 12816 chassis is reload.

Workaround: Reload the Cisco 12816.

- CSCsg75241

Symptoms: GSR Engine 2 -8xOC3 ATM LC ports stops traffic forwarding with %QM-4-STUCK error.

Conditions: This symptom has been observed when there are bad packets hitting the GSR router, especially those packets with sizes that GSR's ATM SAR device can not handle. They include the sizes 1 byte to 4 bytes small. Unexpected large packets also might cause similar issues. L2VPN configuration exists on the Engine 2 ATM line-card and there are AAL0 VCs (encapsulation aal0). Please note that these packets are errored or corrupted packets and are not intentionally generated by regular traffic.

Workaround: Reload the Engine 2 ATM line-card.

- CSCsg75269

Symptoms: QM-STUCK or QM-BUFFER-SANITY messages are logged continuously on Engine 2 ATM Line card of Cisco 12000 series router. The traffic in the egress direction of this line-card is impacted and all packets are dropped on the Tx BMA.

It is very difficult to execute any command on the line card due to slow response and the above continuous messages.

LC reset due to "RP unicast ping time-outs".

Conditions: This symptom has been observed when there are bad packets hitting the ATM SAR device, especially those packets with sizes that ATM SAR device can not handle. They include the sizes 1 byte to 4 bytes small. Unexpected large packets also might cause similar issues. L2VPN configuration exists on the Engine 2 ATM line-card and there are AAL0 VCs (encapsulation aal0). Please note that these packets are errored or corrupted packets and are not intentionally generated by regular traffic.

Workaround: Reload the Engine 2 ATM line-card.

- CSCsg76011

Symptoms: Certain packet corruption which changes bufhdr length to 0 can result in a line card traffic disruption because of Alpha errors.

Conditions: This symptom has been observed with a Cisco 12000 router, Engine-3 line card, and multicast traffic.

Workaround: There is no workaround.

- CSCsg80310

Symptoms: Egress packet rate is doubled due to fragmentation. This can be seen in the output of the **show ip mroute vrf vrf-name active** command.

Conditions: This symptom has been observed only in multicast VPN environment for 1500 bytes packets when the egress linecard is based on Layer 3 Forwarding Engine 3 or 5.

Workaround: Increase the MTU of the egress interface (towards the CE) to 1501.

- CSCsg80414

Symptoms: MPLS OAM ping and traceroute to TE tunnel tail fail at penultimate hop

Conditions: This symptom has been observed when the penultimate hop P router has 4 port OC48 E4 line card. The egress line card E4+ is 4 port OC48. Move the egress fiber to another port on the ingress E4 line card and problem is gone.

Workaround: There is no workaround.

- CSCsg82004

Symptoms: SPA-1XCHSTM1/OC3 interface does not come up on physical loopback

Conditions: This symptom has been observed with a physical loopback.

Workaround: There is no workaround.

- CSCsg95313

Symptoms: A router with a DPT uplink is stuck in reload loop. Every time the router reloads a crash occurs.

Conditions: This symptom has been observed when some DPT uplinks when using images that have the latest version of the Rx FPGA (for example: 32.SY1, 32.S5).

Workaround: There is no workaround.

- CSCsg95894

Symptoms: The GSR systems incorrectly detect removal of all cards in the system, including the Active RP. If a Standby RP is present it will automatically assume Active role but it will also not see any other cards in the system. User-initiated or automatic system reload attempts will fail, the system being unable to come back up. Only a power cycle of the entire chassis will restore the system to normal operation - the only difference from the case in which a _permanent_ h/w failure affecting the MBUS CAN, not covered by this bug.

Conditions: This symptom has been observed in extremely rare occurrences, with no apparent reason. The only theory that could explain the symptoms and was successfully simulated in the lab is a temporary failure in the MBUS h/w circuitry.

Workaround: No workaround can presently prevent the service interruption. A manual power cycle of the chassis would restore normal operation.

Further Problem Description: The MBUS is the backbone of the GSR - a shared CAN bus connecting all cards in the system. A jam condition on this bus would affect communication between all cards, effectively bringing the system down with at least the symptoms described above. The jam condition can happen only if a permanent or temporary failure occurs in the MBUS circuitry. There is nothing the software can do if the failure is permanent, not even a chassis power cycle would correct the problem. Sequenced physical OIRs for all cards in the system would be the only way of identifying the bad one. But at least in some of the temporary failure cases there are chances of software-driven, automatic recovery, which would reduce or maybe even eliminate completely the service interruption. This bug was raised to track the implementation of this particular recovery solution.

- CSCsg96495

Symptoms: An errmsg of type: IDBINDEX_SYNC-3-IDBINDEX_ENTRY_SET for an interface. And “show idb” shows an if-index value of -1 for one or more IDBs on either the Standby or Active RP.

If this happens on a Standby RP there is no affect on traffic. However if the RP switches over to become Active it will prevent traffic from flowing on the affected interfaces.

Conditions: This symptom has been observed when a platform has a bug such that OIR insertion notifications are synced to the Standby RP before the corresponding interface index values have been synced. The normal order is to always guarantee the index values arrive first.

Workaround: A workaround if this happens on an HA protected Active RP (which affects traffic) is to check whether the Standby RP has good if-index values for all interfaces by running the "show idb" EXEC command on the Standby RP. If so, then do an RP switchover, so the RP with good interface indexes becomes the Active RP.

If the Standby RP shows this symptom, the workaround is to reload the Standby RP and check that after it comes up it has good interface index values, which should happen in most cases.

Further Problem Description: This DOTS is to provide a platform-independent code workaround that allows the interface index values to self-recover after the correct if-index values are synced to the Standby RP.

If the condition is seen on an Active RP, this DOTS fix will allow it to recover following an OIR deletion/insertion rather than remaining in the error condition.

The root-cause of the incorrect syncing order will still need to be fixed by the platform that has this symptom. But this DOTS will lower the severity by allowing it to self-recover in most cases on its own without user intervention.

- CSCsg99129

Symptoms: Submitting the **clear counters** command crashes the 6CT3-SMB linecard.

Conditions: This symptom has been observed when entering the **clear counters** command.

Workaround: There is no workaround.

- CSCsh55026

Symptoms: After RPR+ forced switchover, traffic is no longer passed across the affected frame-relay subinterfaces on the CT3 SPA. Commands run on SPA LC indicate the incorrect mapping of if_number.

Conditions: This symptom has been observed with RPR+ switchover, BGP running, routes injected and 180,000 routes set up.

Workaround: Reload the slot containing the CT3 SPA.

Wide-Area Networking

- CSCek49202

Symptoms: When an attempt to move an interface from one multilink group to another fails due to platform-specific limitations, it leaves the interface in an invalid state. The **multilink-group** command still appears in the interface configuration, but the interface does not appear in the output of **show ppp multilink**.

Conditions: This symptom can occur on platforms that support distributed implementations of multilink (such as the Cisco 7500, Cisco 7600, Cisco 10000, or Cisco 12000), and the platform does not allow the interface to be added to a multilink group for some reason (e.g. resource constraints).

Workaround: Use the **no multilink-group** command to remove the interface from its current multilink group before adding it to a new one.

Resolved Caveats—Cisco IOS Release 12.0(32)S5

Cisco IOS Release 12.0(32)S5 is a rebuild of Cisco IOS Release 12.0(32)S. The caveats listed in this section are resolved in Cisco IOS Release 12.0(32)S5 but may be open in previous Cisco IOS releases. This section describes only severity 1, severity 2, and select severity 3 caveats.

Basic System Services

- CSCsd55847

Symptoms: A ping does not go through completely.

Conditions: This symptom is observed after you have entered the **microcode reload** command.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface.

IP Routing Protocols

- CSCsc35663

Symptoms: Mal-formatted MDT updates with 0 masklen are sent to the neighbor PE. It is denied, and PIM neighborship cannot be established properly over the MVPN GRE tunnel.

Conditions: This BGP update issue with MDT AF is observed on an IOU setup.

Workaround: Issue the **clear ip bgp neighbor PE ip address ipv4 mdt in** on PE.

- CSCse64256

Symptoms: When a First Hop Router receives (S,G) stream for an Embedded RP group, the router crashes while trying to send register packets.

Conditions: This symptom has been observed on a First Hop Router.

Workaround: There is no workaround.

Miscellaneous

- CSCdu09372

Symptoms: The Route Switch Module (RSM) may fail to boot or reboots repeatedly.

Conditions: This symptom is observed when Null0 interface is specified as the default output in local policy routing.

Workaround: There is no workaround.

- CSCeb13026

Symptoms: The Cisco IOS TACACS+ is not able to communicate with a TACACS+ server.

Conditions: This symptom occurs when no authentication and encryption key has been configured.

Workaround: Define a key.

- CSCec18644

Symptoms: A Cisco router configuration causes a large memory leak.

Conditions: This symptom has been observed when the following two configuration commands are active at the same time:

1. service compress-config
2. boot config c:auto_config_slot09 nvbypass

This symptom causes a large memory leak each time the configuration is written. If neither configuration or only one configuration command is present, then there will not be a memory leak. This symptom affects RPM-PR and RPM-XF platforms.

Workaround: Do not use the two commands together.

- CSCek13657

Symptoms: The following error message may be generated when a router boots:

```
%SYS-2-NULLCHUNK: Memory requested from Null Chunk -Process= "Init", ipl= 3, pid= 3  
with an accompanying traceback.
```

Conditions: This symptom is platform- and release-independent and occurs when the router boots.

Workaround: There is no workaround. However, proper system operation is not affected.

- CSCek45032

Symptoms: A E5 or E5+ line card crashes when applying a 40K ACL which is used to filter the rate-limit statement.

Conditions: This symptom has been observed on a Cisco 12000 series Internet router which contains 40K ACL filters on E5 or E5+ CAR statements.

Workaround: There is no workaround.

- CSCek56147

Symptoms: The counters for the **show ip mroute vrf vrf-name count** command and the **show ip pim vrf vrf-name interface count** command show huge counts in the decapsulation direction.

Conditions: This symptom has been observed on systems running Cisco IOS Release 12.0(32)S4 after the core facing interface on the local OR remote PE is flapped.

Workaround: The **clear ip pim vrf vrf-name count** command would clear this condition for the respective counters. For the **show ip mroute vrf vrf-name count** command counters, either the route should be cleared or timed out for these counters to reset.

- CSCsa56129

Symptoms: IP explicit path configuration change may not sync to the standby RP.

Conditions: This symptom has been observed during a configuration change.

Workaround: There is no workaround.

- CSCsd43679

Symptoms: Reloading a dual-rp router, where engine 0 6xCT3 or engine 3 1xChOC12 is in the hw-module shutdown state, may cause %IDBINDEX_SYNC-3- IDBINDEX_ENTRY_LOOKUP and some tracebacks.

Conditions: This symptom has been observed on a Cisco 12000 series dual-prp router running Cisco IOS Release 12.0(32)S.

Workaround: There is no workaround.

- CSCsd46103

Symptoms: Multicast states are created but Multicast routing instances are not found on the line card.

Conditions: This symptom has been observed when the hosts join the multicast group.

Workaround: There is no workaround.

- CSCsd47671

Symptoms: A Cisco 7200 series router that is running Cisco IOS Release 12.3(17) may experience an Output stuck condition on PVCs that are running on PA-A3-8T1-IMA. The condition results in all traffic over affected PVCs ceasing to pass.

show queueing int atm1/ima0 may report:

```
Interface ATM1/ima0 VC 1/41
Queueing strategy: fifo
Output queue 40/40, 9156 drops per VC
```

Conditions: See the following:

1. Issue is reproducible in TAC Labs that are running Cisco IOS Release 12.3(17a).
2. Issue is not reproducible in TAC Labs that are running Cisco IOS Release 12.4(5a).
3. During the problem, after interfaces are wedged, doing the **shut** command followed by the **no shut** command on the logical IMA interface results in the interface showing down/down (disabled).

Condition appears in all Cisco IOS versions that contain the fix for CSCee20451.

Workaround: See the following:

1. Reload Cisco 7200 series router.
2. Run Cisco IOS image that does not include the fix for CSCee20451.

- CSCsd48309

Symptoms: The MFR bundle flaps after taking out all of the members and then adding them back.

Conditions: This symptom has been observed when taking out all of the members and then adding them back.

Workaround: Reload the SPA.

- CSCse28337

Symptoms: A 2OC192 Engine6 line card always samples less ingress netflow from total input packets.

Conditions: This symptom is observed on an Engine6 2OC192 line card.

Workaround: There is no workaround.

- CSCse45358

Symptoms: After a router reloads, traffic with frame size of 1615 bytes may not pass through MLPPP bundle configured with Link Fragmentation and Interleaving (LFI).

Conditions: This symptom is observed on a Cisco 12000 series router that is running the c12kprp-p-mz image of Cisco IOS Release 12.0(32)SY.

Workaround: Remove LFI on both sides of the MLPPP link and re add LFI to both sides of MLPPP link simultaneously.

- CSCse48477

Symptoms: The hardware addresses of 4xGE are varying every time when attempting to perform RPR+ switchover.

Conditions: This symptom has been observed with the following conditions:

- Fully populated Cisco 12416 chassis
- Dual PRP-2 with RPR+ HA mode
- Tetra line card
- MVPN scalable configuration
- RPR+ force switching

Workaround: There is no workaround.

Additional Notes: If we take out the standby RP and execute the **show gsr chassis detail** command, with single RP and still we are not able to read then the problem may be caused by a misprogrammed EEPROM, otherwise it should be CSCse48477.

- CSCse48998

Symptoms: The router crashes.

Conditions: This symptom has been observed when applying a service policy on E4P Gigabit subinterface with Xconnect.

Workaround: There is no workaround.

- CSCse92149

Symptoms: Adding uRPF to the main Frame Relay interface will break sub- interfaces added afterwards. Removing uRPF from the main interface does not clear the symptom.

Conditions: This symptom has been observed on a Cisco 12410 router with a SIP- 601/CT3 SPA line card running Cisco IOS Release 12.0(32)S3.

Workaround: uRPF should not be applied to a main interface that is supporting sub-interfaces, so avoiding this negative scenario will prevent this symptom. If this scenario is encountered, shutting down and restarting the sub- interface should clear the issue.

- CSCse92391

Symptoms: Incorrect Legacy QoS behaviour occurs on subinterfaces configured on Engine 0 and Engine 1 line cards. When this error occurs, QoS appears to be applied even though it hasn't been configured.

Conditions: This symptom has been observed when configuring a new subinterface on a line card after another subinterface with QoS was deleted.

Workaround: Reload the line card in question.

- CSCse93643

Symptoms: Unexpected TE FRR status occurs. TE tunnel traffic is not forwarded on expected interfaces. FRR is active when it should have returned to Ready mode. The FRR state on the RP is not the same as the line cards, as seen by the following commands:

show mpls traffic-eng fast-reroute database

exec

slot *slot-number*

show mpls traffic-eng fast-reroute database

Conditions: This symptom has been observed on Cisco 12000 Series Internet Router distributed platforms with Interface or Hello events that activate TE FRR. With TE tunnels, manually configured tunnels are affected, but the symptom is more likely to be seen with auto-tunnel primary and auto-tunnel mesh.

Workaround: There is no workaround. The router must be reloaded, or each line card reset.

Further Problem Description: There is a data table in memory on the RP and each LC that contains the current status and forwarding information for FRR protection. The data should always be in sync, so that the RP and line cards have the same FRR state, but with this symptom, the tables on the line cards become out of sync with the RP, and contain stale information. The situation becomes worse over time as more stale entries are created. The tunnel items are not deleted from the TFIB/FRR database when a tunnel ID is reused by the RP to signal a tunnel to a new destination. These old entries may get chosen for FRR instead of the latest, correct ones, causing incorrect FRR forwarding and incorrect FRR status. Because the tunnels involve multiple destinations and multiple interfaces, with out-of-date forwarding, interface transitions on any TE interface may cause unexpected traffic on any other TE interface. Also, because it is not expected that multiple entries exist for a single tunnel ID, it is difficult to predict which entries will be used, and whether or not an interface event will result in incorrect forwarding.

- CSCse96746

Symptoms: SIP401, SIP501, SIP600, or SIP601 reloads after any of these conditions:

- A SPA OIR
- Interface shutdown and restart
- Any other condition leading to FRR activation.

Conditions: This symptom occurs only during the following conditions:

- Incoming traffic is MPLS.
- Primary link of FRR goes down and backup link becomes active.
- The backup link is through an interface on an E2, E4, E4+, or E6 card.
- ToFab QOS and/or FrFab QOS are configured on an E2, E4, E4+, or E6 card.
- The symptom happens only in Cisco IOS Release 12.0(32)S release and above and is not applicable to Cisco IOS Release 12.0(31)S.

Workaround: Ensure that backup links are not E2, E4, E4+, or E6 under these FRR conditions.

- CSCse97331

Symptoms: Disabling scrambling on an OC48-POS SPA will be lost if a router reload occurs, resulting in a failed link.

Conditions: This symptom is observed with SPA-2xOC48POS/RPR in an Engine 5 Cisco 12000-SIP-601 or Cisco 12000-SIP-600 line card in a Cisco 12000 series router. Additional testing indicates that all supported POS SPA's are affected as shown in this list:

- 2xOC3c POS SPA
- 4xOC3c POS SPA
- 1xOC12c POS SPA
- 1xOC48c POS/RPR SPA
- 4xOC48c POS/RPR SPA
- 1xOC192c POS/RPR SPA

Workaround: There is no workaround.

- CSCse98404

Symptoms: When you apply an input service policy to an AToM PVC, a router may reload and generate the following error message and traceback:

```
Unexpected exception to CPUvector 300, PC = 119B6D0
-Traceback= 119B6D0 118E2F8 5952270 118FDC4 11B7680 11B78EC 236988 24BDD4
2E95CC
```

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(32)S3 but is platform- and release-independent. The symptom occurs when you enter the following commands:

```
Router(config)# interface x/y.z point-to-point
Router(config-subif)# no ip directed-broadcast
Router(config-subif)# no atm enable-ilmi-trap
Router(config-subif)# pvc a/b l2transport
Router(cfg-if-atm-l2trans-pvc)# encapsulation aal5
Router(cfg-if-atm-l2trans-pvc)# xconnect a.b.c.d xy encapsulation mpls
Router(cfg-if-atm-l2trans-pvc-xconn)#
Router(cfg-if-atm-l2trans-pvc-xconn)# service-policy test
```

Workaround: There is no workaround.

- CSCsf04754

Multiple Cisco products contain either of two authentication vulnerabilities in the Simple Network Management Protocol version 3 (SNMPv3) feature. These vulnerabilities can be exploited when processing a malformed SNMPv3 message. These vulnerabilities could allow the disclosure of network information or may enable an attacker to perform configuration changes to vulnerable devices. The SNMP server is an optional service that is disabled by default. Only SNMPv3 is impacted by these vulnerabilities. Workarounds are available for mitigating the impact of the vulnerabilities described in this document.

The United States Computer Emergency Response Team (US-CERT) has assigned Vulnerability Note VU#878044 to these vulnerabilities.

Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-0960 has been assigned to these vulnerabilities.

This advisory will be posted at:

<http://www.cisco.com/warp/public/707/cisco-sa-20080610-snmpv3.shtml>

- CSCsf05948

Symptoms: After failover of the primary RP to secondary RP, errors occurs on slot0 which is a 4 port Gigabit Ethernet Edge Engine 3 card on the Cisco GSR and the 4-port card stops forwarding outbound traffic.

```
Slot 0  type  = 4 Port ISE Gigabit Ethernet
        state = IOS RUN   Line Card Enabled
```

Conditions: This symptom has been seen with either a hardware OIR or a redundancy force-switchover command issued to failover the primary to secondary RP. The symptom seems to happen if there is traffic on the ports of the 4-port card.

Workaround: Reloading of slot0 and the 4-port card seems to clear the problem.

- CSCsf07953

Symptoms: The router may reload when process-level packets are sent to multiple interfaces with QoS enabled, and the user attaches or removes QoS policy from one of the interfaces under traffic.

Conditions: The symptom happens when there are continuous streams of process- switched or router-generated packets during the QoS configuration change.

Workaround: Enabling CEF or fastswitching should avoid the problem.

- CSCsf07966

Symptoms: Router may reload when both fastswitched and CEF switched packets and process-level packets are congesting an interface that has QoS enabled.

Conditions: The symptom is seen when the traffic consists of large packet size greater than 512 bytes and is reported on PA-4T/8T+ interface only. It is not seen on channelized interfaces.

Workaround: There is no workaround.

- CSCsf10205

Symptoms: An ISE OC48 or 4xOC12 channelized card may display the error message:

```
EE48-3-QM_ERR_DECODE: FrFab QM_TX_ERRORS qm_oqdq_halted
```

This error will reset the forwarding and queueing ASICs resulting in small traffic disruption.

Conditions: This symptom occurs when the ports are dynamically channelized and/or unchannelized.

Workaround: Micro-reload the line card after channelization or unchannelization.

- CSCsf11182

Symptoms: The output of the **show policy-map interface** *interface-name* **vp vpi input** command for an ATM interface does not show anything and states that the policy is not configured. However, the output of the **show running-config** command does show the service policy for the ATM interface.

Conditions: This symptom is observed on a Cisco router after an RP switchover has occurred twice.

Workaround: There is no workaround.

- CSCsf12388

Symptoms: Packets may reach incorrect destination during MPLS TE Tunnel Flaps.

Conditions: An LSP being reoptimized causes a label to get reused. This may cause the packet to be switched to an incorrect destination for a brief period. This brief period, usually about 1 or 2 seconds, is the time taken for the label for the old prefix to be withdrawn from other routers. It should be noted that the label reuse doesn't always occur.

Workaround: There is no workaround.

- CSCsf17284

Symptoms: Keep the T1 controller in the `up` state, and when reloading the router in the running configuration after the router comes up, the T1 controller has been shut down.

Conditions: This symptom has been observed on Cisco IOS Release 12.0(32)S and Release 12.0(32)SY.

Workaround: To bring the T1 controller up, use the **no shutdown** command on the controller. There is no workaround.

- CSCsf22278

Symptoms: Incorrectly attaching a service policy under the ATM subinterface and then re-adding interfaces with service policies will cause the latter interfaces to not have QoS applied. This can be avoided by correctly adding service policies under the PVC configuration only.

Conditions: This symptom has been observed when applying service policies to the subinterface directly.

Workaround: The issue can be avoided by not applying service policies to the subinterface directly and instead applying the service policies under the PVC configuration. Shutting down and restarting the affected interfaces is required to clear the issue.

- CSCsf26908

Symptoms: A CHSTM1 controller TUG-2 E1 remote alarm does not clear until the controller is shut down. This symptom happens only on an unframed E1.

Conditions: The receiver must be receiving a remote alarm, while the E1 framing is changed from framed to unframed.

Workaround: Enter the **shutdown** command and then the **no shutdown** command on the controller to clear the remote alarm condition.

- CSCsf28948

Symptoms: A 4xOC3 ATM ISE line card stops process packets in the small buffers queue (80 byte queue). All traffic ceases and the ATM PVCs configured over the line card is set to a down/down state. Resetting the LC clears the buffers and resolves the issue, but it reoccurs. There appears to be a slow leak or alternately sporadic bursts of traffic with malformed 80-byte packets that fill the buffer and cause the issue to reappear.

Conditions: This symptom has been observed with Cisco IOS Release 12.0(32)S3.

Workaround: Micro-reload of line card solves the issue temporarily, but it reappears.

- CSCsf32676

Symptoms: Output rate limit is not working for the new rate limit configured for the interface.

Conditions: This happens when an egress line card used does rate limit in the slow path (e.g.: Engine 0 line card). This occurs only when a new rate limit configuration is added after the router is brought up. If the rate limit on the egress is already present during the router bringup, then the issue will not be observed. When Engines that implement rate limit in hardware like E3/E5 are used as the egress, then the issue will not occur.

Workaround: The ingress line card would need to be reset for the new output rate limit configuration on the egress to take effect. If the rate limit on the egress is already present during router bringup, then the issue will not be observed.

- CSCsf99490

Symptoms: The ACL actually applied on a line card interface is different than what is configured on the RP.

Conditions: This symptom has been observed when changing ACLs with the **ip access group** command applied to interfaces of a line card very quickly. The following examples shows the initial configuration and the configuration which has this symptom.

Initial configuration:

```
interface GigabitEthernet 2/0/0
  ip access-group 116 in
interface GigabitEthernet 2/0/1
  ip access-group 116 in
interface GigabitEthernet 2/0/2
  ip access-group 116 in
interface GigabitEthernet 2/0/3
  ip access-group 115 in
```

Changed configuration with issue:

```
interface GigabitEthernet 2/0/0
  ip access-group 115 in
interface GigabitEthernet 2/0/1
```

```

ip access-group 115 in
interface GigabitEthernet 2/0/3
no ip access-group in

```

Workaround: Add a slight delay between interface configuration changes. This example shows the changed configuration which has no issues:

```

interface GigabitEthernet 2/0/0
ip access-group 115 in
<===== Couple of sec delay
interface GigabitEthernet 2/0/1
ip access-group 115 in
<===== Couple of sec delay
interface GigabitEthernet 2/0/3
no ip access-group in

```

- CSCsg03530

Symptoms: On a Cisco 12000-series Internet router running Cisco IOS Release 12.0(32)S or later, a SIP-600 or SIP-601 line card may exhibit the following error and software-switch packets:

Logs:

```

*Sep 13 02:39:55 KST: %QM-2-TCAM_ERROR: TCAM pgm error(46): LC based QOS Mgr failed
*Sep 13 02:39:55 KST: %QM-4-SW_SWITCH: Interface GigabitEthernet3/0/0.36 routed
traffic will be software switched in egress direction(s)

```

Conditions: This symptom occurs when the following are present on the same line card.

1. A policy-map configured on DOWN (but not shutdown) interface and the same policy-map configured on a SHUTDOWN interface.
2. If any UP interfaces also have the policy-map configured, the error may be seen.

Workarounds: There are three separate workarounds. Only one needs to be chosen:

1. Configure a separate policy-map (with different name) on each interface on that LC. The problem is only seen when interfaces are sharing the same policy.



Note This may not be feasible for policies using complex class-maps due to increased resource utilization, especially when ACL matching is used.

2. Ensure SHUT interfaces never have a policy configured. Remove policies before shutting down any interface. Bring interfaces up before applying a policy which is also present on other interfaces.
3. Reload the line card. This needs to be done once each time the router is reloaded (after it comes up completely). If the LC has been reloaded since the most recent router reboot, the problem will not be seen.

Recovery from error:

If the error has already been seen on the router, possible modes of recovery are:

1. Reloading the LC will recover the LC and prevent any further problems while the router remains up. One of the other workaround should also be selected to prevent the symptom when the router is later rebooted.
2. Shut down all affected interfaces. Shut down any interfaces which are in the DOWN state and have the policy attached. Remove the policy from all the shutdown interfaces. Now the policy can be reapplied and interfaces brought back up.

- CSCsg12862

Symptoms: The 4-port engine-3 based (edge engine) gigabit ethernet line card has missing RX side hardware entries when performing the **show ip hardware-m rx vrf vrf-name group IP** command.

Conditions: This symptom has been observed with large scale MVPN setup.

Workaround: There is no workaround.

TCP/IP Host-Mode Services

- CSCsf01137

Symptoms: PAKPRIORITY flag is not set on the LDP TCP session. The **mpls ldp tcp pakpriority** command is configured and LDP session is restarted.

As result LDP TCP session may be prioritized over non important traffic. Consequently, under sustained traffic, LDP TCP packet might be dropped and LDP session reset.

Conditions: PAKPRIORITY is never set for LDP TCP packets.

The LDP session reset has been seen in specific conditions with E4+ and MQC classes matching the **mpls experimental** command (and not the **ip precedence** command).

Workaround: LDP TCP packets are marked with precedence-6 packets, therefore configuring a class matching on precedence 6 traffic will differentiate LDP traffic in a separate class from non important traffic.

Further Problem Description: MQC in combination with E4+ line cards do not allow matching both the **mpls experimental** command and the **ip precedence** command but only one of the two. This situation causes this symptom in the MPLS environment that requires MQC policies to be configured with mpls experimental to match indifferently on IP and MPLS transit traffic.

Resolved Caveats—Cisco IOS Release 12.0(32)S4

Cisco IOS Release 12.0(32)S4 is a rebuild of Cisco IOS Release 12.0(32)S. The caveats listed in this section are resolved in Cisco IOS Release 12.0(32)S4 but may be open in previous Cisco IOS releases. This section describes only severity 1, severity 2, and select severity 3 caveats.

Basic System Services

- CSCeh65692

Symptoms: Spurious memory access errors and tracebacks may be generated on a Cisco AS5800.

Condition: This symptom is observed on a Cisco AS5800 that processes TCPclear calls.

Workaround: There is no workaround.

IP Routing Protocols

- CSCek31478

Symptoms: When you modify an access control list (ACL) by entering the **ip multicast boundary** command, the command may not fully take effect.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S4 or Release 12.0(32)S but appears to be platform- and release-independent.

Workaround: Disable and re-enter the **ip multicast boundary** command.

Alternate Workaround: Enter the **clear ip mroute *** command.

- CSCsb69773

Symptoms: The router may crash.

Conditions: This symptom has been observed following a switchover from the primary RP to the secondary RP.

Workaround: There is no workaround.

- CSCsc00378

Symptoms: Changes in an export map are not picked up by the BGP Scanner.

Conditions: This symptom is observed on a Cisco router that functions as a PE router when you apply an export map to a VRF and when the interface that connects the PE router to a CE router is configured for OSPF.

Workaround: Enter the **clear ip ospf process** command to enable the BGP Scanner to pick up the changes in the export map.

- CSCsc74229

Symptoms: A router may delete the VPNv4 prefixes from the BGP table, even though the counters in the output of the **show ip bgp** command may indicate that the VPNv4 prefixes are present in the BGP table. This situation may cause loss of VPN connectivity.

Conditions: This symptom is observed on a Cisco router that is configured for MPLS VPN and that functions as a PE router.

Workaround: There is no workaround. When the symptom occurs, enter the **clear ip bgp *** command to restore proper operation of the router.

- CSCsc76327

Symptoms: When a VRF route is redistributed into the MP-BGP cloud, a routing loop may occur for the prefix (that represents the VRF route) between the EIGRP cloud and the MP-BGP cloud.

Conditions: This symptom is observed on a Cisco router that functions as a PE router when the following conditions are present:

- The router has EIGRP configured on the link to a CE router.
- The router has a static VRF route that is redistributed into the configuration that is defined by the **address-family vrf vrf-name** command and that is part of the BGP routing process.

Workaround: There is no workaround. Applying a route map with a pre-bestpath option does not resolve the loop.

- CSCsd03383

Symptoms: A route is not installed through an MPLS TE tunnel even though the **tunnel mpls traffic-eng autoroute announce** command is enabled.

Conditions: This symptom is observed on a Cisco router that also has the **mpls traffic-eng multicast-intact** command enabled.

Workaround: There is no workaround.

- CSCsd04704

Symptoms: A router crashes when you enter the **show ip bgp pending-prefixes** command.

Conditions: This symptom is observed on a Cisco router that runs an interim release for Cisco IOS Release 12.0(32)S and that is configured for BGP

Workaround: Do not issue the **show ip bgp pending-prefixes** command.

- CSCsd64173

Symptoms: A router may reload unexpectedly because of a bus error crash after you have removed a **summary-prefix** IPv6 OSPF command.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(18)SXF but may also occur in other releases. The symptom occurs only when the **summary-prefix** IPv6 OSPF command is configured without any **redistribute** commands.

Workaround: Configure a **redistribute** command under the IPv6 OSPF configuration.

- CSCse66732

Symptoms: If Spatial Reuse Protocol (SRP) is used, Enhanced Interior Gateway Routing Protocol (EIGRP) does not respond to the ring drop notification from the interface.

Conditions: This symptom is observed if SRP is used with EIGRP.

Workaround: There is no workaround.

- CSCuk58462

Symptoms: When a route map is configured, routes may not be filtered as you would expect them to be filtered.

Conditions: This symptom is observed on a Cisco router that is configured for BGP and that functions in an MPLS VPN environment.

Workaround: There is no workaround.

Further Problem Description: The symptom does not occur for redistributed route maps.

Miscellaneous

- CSCef77681

Symptoms: A traceback and 100-to 600-ms traffic loss may occur on an Engine 3 line card while FRR rewrite and reoptimization occurs.

Conditions: This symptom is observed on a Cisco 12000 series that functions as a PE router and that has a multihop TE tunnel to a P router. The multihop TE tunnel is configured for FRR protection and VPNv4 traffic. The symptom may be platform-independent.

Workaround: There is no workaround.

- CSCeh55186

Symptoms: MPLS TE LSPs may not come up and may remain stuck in the RSVP signaling proceeding state.

Conditions: This symptom is observed on a Cisco router when the MPLS TE LSPs are processed over inter-autonomous system broadcast links on which the **passive-interface** command is enabled.

Workaround: There is no workaround.

Further Problem Description: The **passive-interface** command contains the router ID of the remote Autonomous System Border Router (ASBR). A PATH message that leaves the passive interface of the Cisco router is sent to remote ASBR, causing an ARP request to be initiated for remote ASBR. However, there is no response to the ARP request (when there is no proxy configured for ARP), preventing the PATH message from reaching the remote ASBR.

- CSCei01953
Symptoms: There is no **show** command to view if an STS-1 in loopback mode on a CHOC12/DS1 line card.
Conditions: This symptom has been observed when an STS-1 in loopback mode on a CHOC12/DS1 line card.
Workaround: There is no workaround.
- CSCek25192
Symptoms: Error Message keep clogging the console and makes it useless.
Conditions: This symptom has been observed when configuring police percent.
Workaround: There is no workaround.
- CSCek28317
Symptoms: The line card resets when the interface gets flapped.
Conditions: This symptom has been observed with nCmD configured on the main interface when running Cisco IOS Release 12.0(32)S. It is a timing issue and does not happen all of the time. The interface flaps causes nCmD configuration to update on the line card. Due to some timing issue, the update events sequence does not get to the LC properly. Therefore, LC resets on invalid memory access. The symptom usually occurs with a large nCmD configuration, since it generates more update events which would have a higher chance to get wrong orders to the LC. Interface flapping is not the only trigger. Modifying the QoS configuration, shutting down and restarting the main interface or sub interface, and any events triggering the nCmD configuration to be updated on the LC can cause this issue.
Workaround: There is no workaround.
- CSCek30965
Symptoms: Second RP might die due to the missing OIR status.
Conditions: Remove the RP when the main RP is present, do the switch over, and then replace the card.
Workaround: There is no workaround.
- CSCek44427
Symptoms: An interface of a T3/E3 serial SPA passes traffic even though the output of the **show controller** command shows that there is a “Loss of Frame” alarm. When you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface of the SPA, the alarm is not cleared.
Conditions: This symptom is observed on a Cisco platform that is configured with a T3/E3 serial SPA.
Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface at the remote end.
Further Problem Description: The symptom does not affect proper operation of the platform or the traffic. However, the incorrect alarm status may affect network management utilities.
- CSCek44541
Symptoms: PIM sessions fail to come up over a Data Multicast Distribution Tree (MDT).
Conditions: This symptom is observed on a Cisco router that functions as a PE router after you have entered the **clear ip bgp *** command.

Workaround: Enter the **clear ip mds linecard linecard-slot-number** command. For the *linecard-slot-number* argument, enter the core-facing slot.

- CSCek45970

Symptoms: In unidirectional mode, an Automatic Protection Switching (APS) switchover from a protect channel to a working channel may fail because the interface of the working channel remains in the up/down state.

Conditions: This symptom is observed on a Cisco 12416 that runs Cisco IOS Release 12.0(32)S3 and that has two redundant 1-port channelized OC-48 POS ISE line cards that are configured for APS.

Workaround: There is no workaround.

- CSCek49119

Symptoms: On an Engine 3 CH/OC12 card configured for MLPPP, when MTU is mismatched between the two ends, shutting down and restarting causes MTU to be negotiated. However, this action causes buffer recarving, which is undesirable.

Conditions: This symptom has been observed when MLPPP configured mismatched MTU values, such that the new MTU value would be one that triggers a recarve.

Workaround: Match the MTU values on both sides on the interface

- CSCek49158

Symptoms: Changing an MTU value on an interface may cause the RP to trigger buffer recarve unexpectedly.

Conditions: This symptom has been observed when changing the MTU value using the **mtu bytes** command. The new *bytes* value may or may not trigger the buffer recarve, and this behavior needs to be characterized.

Workaround: There is no workaround.

- CSCsa72313

Symptoms: The following error messages may be generated on a router that has IP ACL enabled:

```
%SYS-2-INSCHED: suspend within scheduler
-Process= "<interrupt level>", ip1= 3
-Traceback= 40525388 40628848 4060AED4 403F15BC 403F34F8 403F37EC 400901C8
4008E730 406A0EEC 40621120
```

Conditions: This symptom is observed on a Cisco router such as a Cisco 7200 series, Cisco 7304, and Cisco 7500 series when a Turbo ACL compilation is configured along with an ACL on an ingress interface and when traffic passes through the ingress interface. The symptom does not affect the Cisco 10000 series.

Workaround: There is no workaround.

- CSCsc83817

Symptoms: When MPLS-aware NetFlow is properly configured, it may not capture MPLS-labeled traffic.

Conditions: This symptom is observed on a Cisco router when MPLS-aware NetFlow is configured via the **ip flow-cache mpls label-position label-position-1** global configuration command and when NetFlow is enabled on the interface via the **ip route-cache flow** interface configuration command.

When MPLS traffic passes over the interface that is configured to capture MPLS-aware NetFlow statistics, MPLS-aware NetFlow should capture label information for the traffic flow, but it does not because the MPLS switching vectors are not properly updated. You can verify this condition in the

output of the **show mpls interfaces** privileged EXEC command. The interface that is configured to capture MPLS-aware NetFlow statistics should show “Feature” switching vectors, but instead shows “Fast” switching vectors:

Expected command output:

```
Interface Ethernet 2/0/1
  IP labeling enabled (ldp):
    Interface config
  LSP Tunnel labeling enabled
  BGP labeling not enabled
  MPLS operational
  Optimum Switching Vectors
    IP to MPLS Turbo Feature Vector
    MPLS Feature Vector
  Fast Switching Vectors:
    IP to MPLS Fast Feature Switching Vector
    MPLS Feature Vector
  MTU = 1500
```

Actual command output:

```
Interface Ethernet 2/0/1
  IP labeling enabled (ldp):
    Interface config
  LSP Tunnel labeling enabled
  BGP labeling not enabled
  MPLS operational
  Optimum Switching Vectors
    IP to MPLS Turbo Vector
    MPLS Turbo Vector
  Fast Switching Vectors:
    IP to MPLS Fast Switching Vector
    MPLS Turbo Vector
  MTU = 1500
```

Workaround: Re-initialize the switching vectors by flapping the interfaces. Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface that is configured to capture MPLS-aware NetFlow statistics.

First Alternate Workaround: Re-initialize the switching vectors by toggling MPLS. Enter the **no mpls ip** interface configuration command followed by the **mpls ip** interface configuration command on the interface that is configured to capture MPLS-aware NetFlow statistics.

Second Alternate Workaround: Re-initialize the switching vectors by toggling any MPLS debug mode. For example, enter the **debug mpls packets** command followed by the **no debug all** privileged EXEC command.

- CSCsc90843

Symptoms: A router that is configured with a multilink bundle may reload unexpectedly with the following error message:

```
%ALIGN-1-FATAL: Illegal access to a low address
```

Conditions: This symptom is observed on a Cisco router when you attempt to remove a service policy from a multilink interface.

Workaround: There is no workaround.

- CSCsc96270

Symptoms: Packets with a size greater than 604 bytes are not received from an ISE line card. This situation is caused by the depletion of buffers, as indicated in the output of the **show controller tofab queue** command.

Conditions: This symptom is observed rarely on a Cisco 12000 series and may be related to corrupt or unidentified traffic.

Workaround: Reload the ISE line card.

- CSCsd12203

Symptoms: On a Cisco 7500 router, the standby may reload with CCB PLAYBACK errors when the standby boots up.

Conditions: This symptom has been observed on a Cisco 7500 HA setup.

Workaround: There is no workaround.

Further Problem Description: There is no functional impact.

- CSCsd13490

Symptoms: An Engine 2 line card may crash when it receives multicast traffic that is not punted to the CPU of the line card but switched by the PSA memory of the line card.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(27)S or a later release when the Engine 2 line card is configured with the wrong PSA memory and when you enable multicast hardware acceleration by entering the **hw-module slot slot-number ip multicast hw-accelerate** command.

Workaround: Disable multicast hardware acceleration on Engine 2 line card.

- CSCsd16581

Symptoms: An Engine 3 or Engine 5 line card may crash while processing packets for Output Sampled NetFlow.

Conditions: This symptom is observed on Cisco 12000 series when Output Sampled NetFlow is enabled on the Engine 3 or Engine 5 line card and when packets are sampled that are not aligned to a 2-byte boundary.

Workaround: Disable Output Sampled NetFlow.

- CSCsd21134

Symptoms: A Cisco 12000 series line card may crash while processing packets that are not aligned to a 4-byte boundary.

Conditions: This symptom is observed when the packet is processed in the CPU of the line card.

Workaround: There is no workaround.

- CSCsd45425

Symptoms: MLPPP interfaces may fail to ping the far end after initial configuration of the bundle. Additionally, the IP address of the directly- attached MLPPP interface will not appear in the routing table.

Conditions: This symptom has been observed with multilink PPP interface(s) configured on the router.

Workaround: There is no workaround.

- CSCsd46323

Symptoms: The standby RP reboots when you perform an OIR of an active VIP that is installed in any slot of the router.

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS interim Release 12.4(7.10) and that is configured for RPR, RPR+, or SSO. The symptom may also affect other releases.

Workaround: There is no workaround.

- CSCsd59330

Symptoms: Applying the **rate-limit output** command to an Engine 0 DS3 subinterface will cause the output bytes counter to not account for traffic passing across any subinterface on the interface that is not part of a VRF.

Conditions: This symptom has been observed when using the **rate-limit output** command.

Workaround: Do not use the **rate-limit output** command.

- CSCsd64707

Symptoms: There are 3 Multilink PPP (MLPPP) and 3 Multilink Frame Relay (MLFR) at 12 links per bundle and 11 HDLC serial interfaces on one SPA-1XCHSTM1/OC3. All MLPPP bundles are up/down on R1 when a cable is physically removed, an SSO switchover performed, and the cable inserted on R1. All MLPPP bundles are up/up on R2.

Conditions: This symptom has been observed when physically removing the cable, doing an SSO switchover, and inserting the cable with traffic running.

Workaround: Enter a **shutdown** and **no shutdown** command on the MLPPP bundles and the bundles will come up.

- CSCsd65902

Symptoms: Some of the thousands of L2TPv3 sessions are not forwarding traffic. The number of affected VCs varies but is usually within a range of 5 to 10.

Conditions: This symptom has been observed with scaled L2TPv3 configuration, with up to 8000 L2TPv3 sessions.

Workaround: Flap the Attachment Circuit (AC) port.

- CSCsd67457

Symptoms: When applying a policy map as in the following example, the system rejects the configuration.

```
policy-map multi-line
  class class-A
    police rate 20000000
      conform-action transmit
      exceed-action drop
```

! note that policing actions are configured on separate lines in this example

The following error message is displayed:

```
%Error: Multi-action police command not supported on interface GigabitEthernet0/0/0
```

Conditions: This symptom has been observed when the police statement is entered on separate lines.

Workaround: Enter the police statement on a single line rather than on separate lines. For example:

```
policy-map single-line
```

```
class class-A
  police rate 20000000 conform-action transmit exceed-action drop
! note that policing actions are configured on one line in this example
```

- CSCsd84951

Symptoms: A VIP may experience a reset due to a bus error (CPU signal 10) after an interface flap.

Conditions: This symptom occurs under normal operation.

Workaround: There is no workaround.

- CSCsd84974

Symptoms: Loss of most of the configuration of a single Multilink PPP or Multilink FR bundle on an RPR+ or an SSO switchover except for the following commands:

- **multilink-group**
- **ppp multilink**
- **ppp chap**
- **frame-relay multilink**
- **frame-relay interface-dlci**
- **frame-relay intf-type**
- **frame-relay lmi-type**
- **ip vrf forwarding**
- **mpls traffic-eng tunnels**
- **ip rsvp bandwidth**

Conditions: The symptom has been observed upon associating hardware with a previously configured multilink bundle (when adding the first link in the bundle), in a router which contains many interface bundles. The symptom is exacerbated when QoS policies are configured. The symptom has been seen when an RP switchover occurs shortly after the first link is added to one or multiple bundles.

Workaround: Manually reapply the configuration to the bundle in question. The symptom should be confined to one bundle only.

- CSCsd93343

Symptoms: Serial interfaces associated with MFR bundles on CT3 SPA may not come back up in service after a physical online removal and insertion.

Conditions: This symptom is observed on a Cisco 12000 series router that runs the gsr-p-mz image of Cisco IOS Release 12.0(32)S2.

Workaround: Enter the **microcode reload sip-601 slot** command.

- CSCsd94142

Symptoms: If a Cisco 12000 series Internet router is configured as a router in a large scale configuration, sometimes one or more line cards can reload silently during switchback from default standby PRP (now in active role) to default primary PRP (now in standby role).

Conditions: This problem is observed in Cisco IOS Release 12.0(32)S2 and later releases.

Workaround: There is no workaround. However, waiting until the CPU utilization has decreased to below 50% will severely reduce the possibility of this problem occurring.

- CSCsd94285

Symptoms: The following traceback may be seen when reloading a sip-601:

```
%EELC_QOS_RES_MGR-3-HW_IDB_INDEX_TO_TX_PORT_MAPPING_FAILED: Mapping of
hwidb_index to tx_port failed. hwidb_index = 63
-Traceback= 40030CB8 406A724C 4069E784 404E3DAC 404E2060 404E24C0 404EEB28
404EF6E4 404EF950
```

Conditions: This symptom is observed on a Cisco 12000 series router that runs the gsr-p-mz image of Cisco IOS Release 12.0(32)S2.

Workaround: There is no workaround.

- CSCse02555

Symptoms: SIP crashes and the following errors and tracebacks are seen:

```
%SPA_PLIM-3-HEARTBEAT: Subslot 2 has experienced an heartbeat failure
```

Conditions: When configuring the **frame-relay interface-dlci** command and assigning or unassigning a mapclass to a data-link connection identifier (DLCI), which has service-policy, SPA connectivity is lost and the above message is displayed.

Workaround: There is no workaround.

- CSCse09498

Symptoms: When you enter the **no shutdown** interface configuration command on an auto-template interface during deployment, some tunnels may be in the up/down state, and the tunnel mode may be GRE instead of the configured tunnel mode of MPLS.

Conditions: This symptom is observed on a Cisco router with about 70 primary MPLS TE tunnels. The symptom occurs when you first enter the **no interface auto-template** command, then you enter the **tunnel mode mpls traffic-eng** command, and finally you paste the template back.

Workaround: Reload the router.

Alternate Workaround: Create an automesh in the following sequence:

```
conf t
access-list 60 permit 10.0.7.3
access-list 60 permit 10.0.1.5
access-list 60 permit 10.0.2.6
access-list 60 permit 10.0.3.7
access-list 60 permit 10.0.5.1
access-list 60 permit 10.0.6.2
access-list 60 permit 10.0.8.12

interface Auto-Template1
 ip unnumbered Loopback0
 no ip directed-broadcast
 tunnel destination access-list 60
 tunnel mode mpls traffic-eng

.....

access-list 60 permit 10.0.7.3
```

```
access-list 60 permit 10.0.1.5
access-list 60 permit 10.0.2.6
access-list 60 permit 10.0.3.7
access-list 60 permit 10.0.5.1
access-list 60 permit 10.0.6.2
access-list 60 permit 10.0.8.12
```

- CSCse12983

Symptoms: If following steps are performed on 2xCT3 SPA and 10x1GE SPA located in E5 12000-SIP-601

- Enter the **hw-module slot shelf-id/slot-number shutdown** command on 2xCT3 SPA.
- Enter the **no hw-module slot shelf-id/slot-number shutdown** command on 2xCT3 SPA.
- Enter the **hw-module slot shelf-id/slot-number shutdown** command on 10x1GE SPA. Before CT3 SPA comes up, the CT3 SPA may get in an out-of-service state.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS interim Release 12.0(32.1)S9

Workaround: Performing the **no hw-module slot shelf-id/slot-number shutdown** command on 10x1GE SPA, or the **microcode reload** command on the SIP-601 may fix the problem.

- CSCse23872

Symptoms: A Cisco 12000 Engine 3 card is used as an IP ingress to classify traffic to different classes using a set of IP standard and extended ACLs. After reaching a stable state, when the ACLs take a substantial part of the TCAM, adding a single line to an ACL used in the class-map may result in the TCAM Mngr merge process on the line card to take 99% CPU for a long time (over 60 seconds), and then crash the card with the following errors:

```
00:14:59: %QM-4-TCAM_ENTRY: Hardware TCAM entry capacity exceeded
00:14:59: %QM-4-SW_SWITCH: Interface GigabitEthernet2/2 routed traffic will be
software switched in ingress direction(s)
SLOT 2:00:14:06: %EE48-5-TM_PROC: TCAM handling fail for features config for
interface: 13
-Traceback= 40030CAC 404B7604 404B76B4 404BA7D4 404BC61C 404BC7C4 404BC8D8
404C7C00 404D197C 404D3684 404C7BB4 404C8800 404C8BA4
00:15:00: %QM-2-TCAM_ERROR: TCAM pgm error(36): Invalid Parameters
```

Conditions: This issue is observed with multiple interfaces on the same line card using service policies with long (over 1000 entries) ACLs.

Workaround: When restarting the line card with the policy-map configured, it boots correctly. Also, removing the QoS policy from all the interfaces, waiting for the TCAM to clear up, then changing the ACL and reapplying the QoS policy on the interface is a valid workaround.

- CSCse29480

Symptoms: Locally originated traffic is not prioritized correctly in specific MQC configuration for MPLS and Engine 4 plus used as the egress LC. Control plane protocols might flap as a result of oversubscription of the default class.

Conditions: This occurs if the policy-map includes a priority class, e.g. to carry voice traffic, and that there is no class mapping precedence 6 or 7 (i.e. the policy map defines mappings only for EXP 6 and 7).

Workaround: There is no workaround other than avoiding oversubscription of the default class.

- CSCse29708

Symptoms: After booting a Cisco 12000 router, Engine3 and Engine4+ line card may get stuck in the MRAM0230 state.

Conditions: This symptom is observed on a Cisco 12000 series router that runs the gsr-p-mz image of Cisco IOS Release 12.0(32)SY and may require physical removal and replacement of the LC if the symptom occurs.

Workaround: Remove automatic mbus agent upgrade by removing the **service upgrade mbus-agent-rom** command from the running configuration, and do a manual mbus agent upgrade by issuing the **upgrade mbus agent** command from the CLI.

- CSCse33664

Symptoms: A multichannel T1 or E1 port adapter may become deactivated when you enter the **invert data** or **crc 16** interface configuration command.

Conditions: This symptom is observed on a Cisco 7500 series that is configured with an RSP4 that contains an R5000 microprocessor.

Workaround: There is no workaround.

- CSCse35036

Symptoms: An interface of a 2-port OC-192 POS Engine 6 line card may stop sampling NetFlow.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S6.

Workaround: Remove NetFlow from the affected interface and then re-apply NetFlow to the interface.

- CSCse35281

Symptoms: Reloading the SPAs in a 12000-SIP-601 line card may causes the 12000-SIP-601 to fail.

Conditions: This symptom is observed in a Cisco 12000-SIP-601 (which has 8xFE, 8xOC12 POS, 2xCT3, & 1xChOC3 SPAs) in a Cisco 12000 series router, running Cisco IOS interim Release 12.0(32.1)S11.

Workaround: There is no workaround.

- CSCse40399

Symptoms: When upgrading the Cisco 12000 series Internet router to Cisco IOS Release 12.0(32)S2, the video streaming deployed through multicast with PBR configured results are heavily degraded with the image frequently frozen on the screen. Other services, like voice, do not seem to be affected.

Conditions: This symptom is observed on a Cisco 12000 series Internet router that is running Cisco IOS Release 12.0(32)S2 and has multicast service and PBR configured on it.

Workaround: Disable the PBR on the interfaces.

- CSCse40424

Symptoms: On a Cisco 12000 series router with SIP-601, there is a possibility to drop important packets, such as keepalives and hellos, as a result of an incorrect configuration.

Conditions: When traffic arrives to an SIP-601, if the egress interface has a glean adjacency, then all the important packets are dropped on the SIP causing protocol flapping.

Workaround: Avoid having glean adjacencies.

- CSCse40966

Symptoms: MLP links on a Cisco GSR running Cisco IOS Release 12.0(32)S2 doesn't come up after ha switchover in SSO mode.

Conditions: This is seen on MLP links created off of serial interfaces on a frost bite card CHOC12/DS1-IR-SC= after ha switchover with mode set to SSO.

Workaround: Remove non-default router global configuration line **aaa new-model** from the router configuration and the problem will not happen.

If the **aaa new-model** command is configure, then one has to shutdown and enable the physical links to restore the MLP link
- CSCse44174

Symptoms: Transient and control traffic of packets that are sized 81-608B could be dropped.

Conditions: This symptom is observed when reloading an Engine 3 line card. Some queues are stuck.

Workaround: There is no workaround.
- CSCse45466

Symptoms: The line protocol on E5 2xOC48 SPA, located in 12000-SIP-600, may not come up after performing the **hw-module slot shelf-id/slot-number shutdown** command followed by the **no hw-module slot shelf-id/slot-number shutdown** command on the SPA.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31.4)SY1

Workaround: Performing the **microcode reload** command on the affected 12000-SIP-600 will fix the problem.
- CSCse50607

Symptoms: Periods of high latency may occur on a Multilink PPP interface, and finally the interface may lock up.

Conditions: This symptom is observed on a Cisco 7600 series when the Multilink PPP interface is configured on a SPA-8XCHT1/E1 that is installed in a SIP-200.

Workaround: Configure multilink interfaces on another line card that does not require insertion in a SIP.

Alternate Workaround: Configure IP load balancing by using two separate E1 links (that is, do not use multilink interfaces).
- CSCse53151

Symptoms: Router crashes at the **show connect** command.

Conditions: The crash occurs if any FRoMPLS or Frame relay local switching connections are present.

Workaround: There is no workaround.
- CSCse66042

Symptoms: Reloading a POS line card with interfaces configured for encapsulation frame-relay IETF and frame-relay subinterfaces, checking the ifIndex for the subinterfaces after the line card restarted it only shows: Incorrect ifIndex for POSxx/y.z

Conditions: The symptom is seen when a line card configured for encapsulation frame-relay IETF and frame-relay subinterfaces is reloaded while the RP remains running.

Workaround: Remove the subinterface configuration and then add it. The ifIndex will again show correct values.

- CSCse69742

Symptoms: On a Engine 5 line card, traffic is dropped on ingress direction without any error report.

Conditions: No special condition is found.

Workaround: There is no workaround.

- CSCse71065

Symptoms: Engine 0, 1 and 2 of a Cisco 12000 suffers from low free memory after upgrading the software image to Cisco IOS Release 12.0(32)S3. Large routing table (like 300,000 BGP routes) may cause memory allocation failure in the mentioned legacy engines, along with configuration of features such as input ACL.

Conditions: This symptom has been observed on a Cisco 12000 with 1GB RPR-1/2, populated with Engine 0, 1, and 2 line cards and when injecting more than 300,000 BGP routes, along with configuring large input security ACLs.

Workaround: There is no workaround.

- CSCse81320

Symptoms: Reconfiguring a T1 on a CT3 SPA installed on a SIP401 with Cisco IOS Release 12.0(32)S3 cases the resulting frame-relay subinterfaces to reflect an incorrect interface number.

Conditions:

- Configure a full T1 on the CT3 with channel-group 0 and time-slots 1-24.
- Configure associated main interfaces with frame-relay encapsulation then configure subinterfaces.
- With all interfaces up and passing traffic, shut down the main interface and then remove the T1 from the T3 controller.
- Recreate the T1 using a different channel-group number and time slots 1-12.

After reconfiguring the main and subinterfaces, the subinterface number still reflects the previous configuration.

Workaround: There is no workaround.

- CSCse82922

Symptoms: Trap "ciscoRFSwacNotif" is not received on Network Management Station after an RPR+ switchover on a Cisco GSR.

Conditions: This symptom has been observed on a Cisco GSR platform running Cisco IOS Release 12.0(32)S3.

Workaround: There is no workaround.

TCP/IP Host-Mode Services

- CSCef52888

Symptoms: Path MTU Discovery (PMTUD) may incorrectly select a higher MTU for an egress interface and may cause BGP to send packets that are larger than the size that the egress interface can support. When this situation occurs, packets are lost and the BGP session may be terminated.

Conditions: This symptom is observed when PMTUD is enabled over parallel links with different MTUs and when the paths in each direction use different links. Some other conditions may also apply, such as CEF and load-balancing being enabled.

Workaround: Enter the **ip tcp mss** command to configure the MSS to be less than the MTUs of all possible egress interfaces, or configure the MTUs of all possible egress interfaces to be same as the MSS.

- CSCek12203

Symptoms: When you enter the **copy ftp disk** command, the copy operation may fail and cannot be terminated, further **copy** commands may fail, and a TCP vty session for the purpose of troubleshooting the situation may fail and cannot be terminated.

Conditions: These symptoms are observed on a Cisco platform when the FIN flag is set in the initial ESTAB message from a neighbor. You must reload the router to recover from the symptoms.

Workaround: Do not enter the **copy ftp disk** command. Rather, enter the **copy tftp disk** command.

Wide-Area Networking

- CSCse75229

Symptoms: Frame Relay LMI crashes due to Address Error (load or instruction fetch) exception.

Conditions: The crash may occur when a Cisco type LMI packet is received which contains an invalid DLCI value.

Workaround: Use q933a or ANSI type LMI.

- CSCse81327

Symptoms: On a Cisco router when a main interface is configured for frame-relay encapsulation with sub-interfaces, when a sub-interface is deleted and re-added, the DLCI information is not re-added to the running configuration and no error message is sent to the CLI to indicate an error.

Conditions: This only occurs if the main interface is shut down. If the main interface is administratively up, this does not occur in our testing. This symptom was introduced between Cisco IOS Release 12.0(30)S and Release 12.0(31)S.

Workaround: Do not provision and rollback sub-interfaces on main interfaces that are shut down. This may not be possible without re-writing customer automated provisioning systems.

Resolved Caveats—Cisco IOS Release 12.0(32)S3

Cisco IOS Release 12.0(32)S3 is a rebuild of Cisco IOS Release 12.0(32)S. The caveats listed in this section are resolved in Cisco IOS Release 12.0(32)S3 but may be open in previous Cisco IOS releases. This section describes only severity 1, severity 2, and select severity 3 caveats.

Basic System Services

- CSCeg11566

Symptoms: Intensive SNMP polling may cause the I/O memory of a router to be depleted.

Conditions: This symptom is observed in rare situations.

Workaround: Reduce the SNMP polling interval, frequency, or rate.

IP Routing Protocols

- CSCsc73598

Symptoms: The IGP metric is not updated to an eBGP peer when there is an IGP- metric change. The BGP peer is not advertising this change after its default timer of 10 minutes.

Conditions: This symptom occurs when a link goes down and the IGP metric to reach the BGP nexthop has changed. When used in a route-map, the **set metric-type internal** value should propagate any MED changes in updates to the BGP peers.

Workaround: Use **clear ip bgp neighbor-address [soft [in | out]]** on the respective router to get the correct metric changes and BGP best path.

- CSCsd66372

Symptoms: A Cisco 12416 router running the Cisco c12kprp-k3p-mz.120-31.S1.bin image restarted.

Conditions: The symptom has been observed when using the Cisco c12kprp-k3p- mz.120-31.S1.bin image. The following message was shown:

```
*Dec 31 14:53:04.667 EST: %SYS-5-CONFIG_I: Configured from memory by console
*Dec 31 14:53:05.163 EST: %SYS-5-RESTART: System restarted
```

```
Unexpected exception to CPUvector 300, PC = 98AFEC
-Traceback= 98AFEC 98AB18 1203EA0 98C3C0 98C678 98D20C 2CE86C
```

Workaround: There is no workaround.

Miscellaneous

- CSCec40013

Symptoms: When using the **redundancy force-switchover** command, a Cisco 12000 router may reload with bus error.

Conditions: This symptom has been observed on a Cisco 12000 router running Cisco IOS Release 12.0(26)S4 and with redundancy SSO enabled.

Workaround: There is no workaround.

- CSCej25402

Symptoms: Standby RP reboots continuously on STANDBY HOT (SSO) mode.

Conditions: This symptom occurs after loading the image and configuring SSO mode.

Workaround: There is no workaround.

- CSCek24285

Symptoms: After configuring a feature bundle on an E3 4x1GE line card and reloading, the line card crashes when IPv6 traffic is processed by the line card.

Conditions: The symptom has been observed after the feature bundle is configured, the line card is reloaded, and as soon as IPv6 traffic is processed by the line card.

Workaround: Remove the feature bundle configuration.

- CSCek34621

Symptoms: After a SPA-capable line card (LC) crash, some or all of the SPAs may occasionally fail to recover. The LC in question will display messages like these, one for every failed SPA (subslot) every 1 to 2 minutes:

```
SLOT 3:00:02:38: %GSRSPA-3-GET_SPA_TYPE_FAILURE: hostType 0x95, slot 3,
subslot 0, rc= 20
-Traceback= 40030CB0 406C4644 406C46C0 406C6A1C 411ECCC0 406C5958 406C7534
406C4E58 406C50C0
```

The affected SPAs appear out of service:

```
Router#sh gsr
SLOT 3:00:02:38: %GSRSPA-3-GET_SPA_TYPE_FAILURE: hostType 0x95, slot 3,
subslot 0, rc= 20
-Traceback= 40030CB0 406C4644 406C46C0 406C6A1C 411ECCC0 406C5958 406C7534
406C4E58 406C50C0
SLOT 3:00:02:38: %GSRSPA-3-GET_SPA_TYPE_FAILURE: hostType 0x95, slot 3,
subslot 0, rc= 20
-Traceback= 40030CB0 406C4644 406C46C0 406C6A1C 411ECCC0 406C5958 406C7534
406C4E58 406C50C0
Slot 3   type   = Modular SPA Interface Card
         state  = IOS RUN    Line Card Enabled
         subslot 3/0: (0x4), status is out of service
<<<<<<<
         subslot 3/1: SPA-1XCHSTM1/OC3 (0x463), status is ok
         subslot 3/2: SPA-2XCT3/DS0 (0x43C), status is ok
         subslot 3/3: Empty
```

Conditions: This symptom has been observed to occur after SPA-capable LC crashes, although such crashes are extremely rare.

Workaround: The following steps should be attempted, in this order, allowing a few seconds then checking the state between steps, until the problem is corrected and the SPA type is detected properly:

1. Execute the **test mbus c2w program slot# default** command.
2. Execute the **hw-module subslot subslot/subcard reload** command.
3. Execute the **hw-module slot number reload** command.
4. Physically remove and re-insert the affected line card.

Further Problem Description: The MBUS transport is not 100% reliable. MBUS message loss is usually extremely rare, but not impossible. If the lost messages happen to be MBUS C2W programming messages, they may cause inconsistencies in the MBUS Agent C2W programming. If the inconsistency happens to affect a single bay's SPA EEPROM C2W device, then it becomes impossible to determine the type of the SPA inserted in that bay. The LC crashes cause very high peaks of MBUS activity, which apparently may cause MBUS message loss (suspecting buffer overrun or out-of-buffer conditions).

- CSCek35844

Symptoms: Continuous traceback with error messages is encountered on removal of an SPA-CH8TE1 card.

Conditions: This symptom has been observed when an SPA-CH8TE1 card is removed from the Cisco 12000 router in an SIP-601 jacket card.

Workaround: Reload the line card.

- CSCek37693

Symptoms: The **speed** command cannot be configured on FE interfaces.

Conditions: This symptom has been seen on a Cisco 7500 series router with a PA- 2FE-TX in a VIP4-80. The FE port is connected to a switch port. If the switch port is set for 10MB and the FE interface is unable to be manually configured with the **speed** command, the FE interface will be in an up/down state.

Workaround: Use the **speed auto** command on the switch port that connects to the FE interface on the router. By using this workaround, you will not be able to throttle the bandwidth to 10MB as desired. The interface will be up/up, and will pass traffic at 100MB.

- CSCsc61288

Symptoms: Performing dual switchover with MDRR configured on an SPA interface shows MDRR queues as unallocated for the **show policy-map** command.

Conditions: This symptom has been observed when configuring MDRR on an SPA interface (POS or SRP) and doing a dual switchover (Main-to-standby and standby-to-Main).

Workaround: Remove the MDRR configuration from the interface and reapply. The MDRR queues reappear.

- CSCsd25480

Symptoms: ISE 10G SPA sends packets with random source MAC addresses.

Conditions: The symptom has been observed intermittently on Cisco IOS Release 12.0(31)S2 with 10G SPAs on SIP-600 LC.

Workaround: There is no workaround.

- CSCsd49782

Symptoms: A VIP may reload unexpectedly when you change the encapsulation from Frame Relay to PPP.

Conditions: This symptom is observed on a Cisco platform that has a VIP that is configured for QoS.

Workaround: There is no workaround.

- CSCsd57040

Symptoms: When the controller of multichannel T3 port adaptor SPA-4XCT3 goes down for a short duration and an alarm occurs, the port adapter does not report the type of alarm.

Conditions: This symptom has been observed on Cisco 7600 series and Cisco 12000 series routers that are configured with a SPA-4XCT3. The port adapter should provide a history table of recent alarm conditions along with a corresponding time stamp to allow for proper troubleshooting.

Workaround: There is no workaround.

- CSCsd62921

Symptoms: An SIP601 line card crashes when shutting down an SPA-8XCHT1/E1 for RPR+ switchover.

Conditions: This symptom has been observed when shutting down an SPA-8XCHT1/E1 on bay 1/1 and performing an RPR+ switchover with traffic running.

Workaround: There is no workaround.

- CSCsd83431

Symptoms: Using the **snmpwalk** command to query the SNMP variable cbQosSetStats in cbQoS-MIB causes a memory leak. The leaked blocks are of 1K size for each single **snmp get** command.

Conditions: The leak only exists if a service-policy is attached under the interface and the service-policy performs a set action as shown in the example:

```
policy-map set-zero
  class set-zero
    set precedence 0
```

Workaround: Do not query the SNMP variable cbQosSetStats in cbQoS-MIB.

- CSCsd91691

Symptoms: A Cisco 12000 E6 line card may crash with sampled netflow configured.

Conditions: This symptom has been observed on a Cisco 12000 E6 line card with MPLS/Multicast traffic.

Workaround: There is no workaround.

- CSCsd94541

Symptoms: The T3 line state may flap when there are no apparent alarms or problems on a channelized T3 to DS0 SPA.

Conditions: This symptom is observed on a Cisco 12000 series when the T3 links are in channelized mode, when the T1 links on the Cisco 12000 series are configured for ESF framing, and when the T1 links on the router at the far end are configured to send T1 FDL ANSI reports.

Workaround: Disable the T1 FDL ANSI configuration on the router at the far end.

Resolved Caveats—Cisco IOS Release 12.0(32)S2

Cisco IOS Release 12.0(32)S2 is a rebuild of Cisco IOS Release 12.0(32)S. The caveats listed in this section are resolved in Cisco IOS Release 12.0(32)S2 but may be open in previous Cisco IOS releases. This section describes only severity 1, severity 2, and select severity 3 caveats.

Basic System Services

- CSCee41892

Symptoms: A VIP4-80 card may fail to load the Cisco IOS software image. When this situation occurs, the following error messages are generated:

```
%DBUS-3-SW_NOTRDY: DBUS software not ready after HARD_RESET, elapsed 13056,
status 0x0
%DBUS-3-WCSLDERR: Slot 2, error loading WCS, status 0x4 cmd/data 0xDEAD pos 97
%DBUS-3-WCSLDERR: Slot 2, error loading WCS, status 0x4 cmd/data 0xDEAD pos 99
%UCODE-3-LDFAIL: Unable to download ucode from system image in slot 2, trying
rom ucode
%RSP-3-NOSTART: No microcode for VIP4-80 RM7000 card, slot 2
```

Conditions: This symptom is observed on a Cisco 7500 series when you enter the **microcode reload** command.

Workaround: There is no workaround.

Further Problem Description: The symptom may also occur because of improperly installed line cards. If this situation occurs, re-install the line cards.

- CSCee84611

Symptoms: An NTP broadcast client may fail to synchronize with an NTP broadcast server if the server cannot be reached from the client.

Conditions: This symptom is observed in Cisco IOS interim Release 12.2(12.11)T or a later release, including Release 12.3. However, the symptom may also occur in other releases.

Workaround: Ensure that the server can be reached from the client.

- CSCsc14034

Symptoms: The active RP crashes during the boot process.

Conditions: This symptom is observed on a Cisco router that is configured for SSO and that has the **snmp mib notification-log default** command enabled.

Workaround: Disable the **snmp mib notification-log default** command.

- CSCsd30334

Symptoms: Latency may be high on a Cisco 7500 series.

Conditions: This symptom is observed a Cisco 7500 series that runs Cisco IOS Release 12.0(31)S when packets are forwarded across a PA-A3 port adapter.

Workaround: There is no workaround.

EXEC and Configuration Parser

- CSCsc76550

Symptoms: The RP may crash with a watchdog timeout error for the IP input process.

Conditions: This symptom is observed on a Cisco 12000 series when you delete a subinterface that processes traffic. The symptom may be platform-independent.

Workaround: Shut down the subinterface before you delete it.

Interfaces and Bridging

- CSCsc01566

Symptoms: An “%ATMPA-3-CMDFAIL” error message and “cm622_vip_parse_cmd” traceback may be generated on the VIP console for an OC-12 ATM interface of a 1-port ATM Enhanced OC-12/STM-4 port adapter (PA-A3-OC12) that is installed in the VIP, and a “setup_vc failed” error message may be generated on the RSP console. This situation causes a VC that is configured on the OC-12 ATM interface to become inactive.

Conditions: This symptom is observed on a Cisco 7500 series when you perform the following steps:

1. You force an SSO switchover.
2. After the new standby RSP comes up, you delete a subinterface from the new active RSP.
3. You create a new subinterface on the active RSP.

At this point, the VC on the OC-12 ATM interface becomes inactive.

Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the OC-12 ATM interface to enable the VC to become active.

- CSCsc30369

Symptoms: A cBus Complex Restart may occur on a Cisco 7500 series when you leave the interface configuration mode after you have changed the encapsulation on a serial interface from HDLC to another encapsulation type such as PPP or Frame Relay.

The maximum datagram for an interface a of low-speed serial port adapter with HDLC encapsulation and an MTU of 1500 is 1528 because the overhead that is added to the MTU is 28. The maximum datagram for an interface a of high-speed serial port adapter with HDLC encapsulation and an MTU of 1500 is 1530 because the overhead that is added to the MTU is 30.

When the encapsulation type is changed, the maximum datagram size may change, which causes an internal MTU change. This situation may cause some packets to be dropped as giants.

Conditions: This symptom is observed after the first change to the type of encapsulation from the default of HDLC to another encapsulation type when you leave the interface configuration mode. Subsequent changes to the type of encapsulation do not cause the cBus Complex Restart.

Workaround for the cBus Complex Restart: There is no workaround for the cBus Complex Restart. An MTU change on a Cisco 7500 series results in a cBus Complex Restart, which usually means a router outage of 15 to 30 seconds or a minute and a half, depending on the Cisco IOS software image that the router is running.

Workaround for the packet drops: Reconfigure the MTU to prevent packet from being dropped as giants.

Further Problem Description: The fix for this caveat ensures the maximum datagram for an interface a of low-speed serial port adapter with HDLC encapsulation and an MTU of 1500 is 1608 to allow for an overhead to the MTU of 108. The maximum datagram for an interface a of high-speed serial port adapter with HDLC encapsulation and an MTU of 1500 is then 1610 to allow for an overhead to the MTU of 110.

- CSCsc71286

Symptoms: The throughput is far below what you would expect on an MFR bundle that is configured on a 8-port multichannel T1/E1 PRI port adapter (PA-MC-8TE1+).

Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.0(31)S2 when the MFR bundle has four T1 links, three of which are shut down. When you generate 2.5 Mbps of traffic to congest the one active link, a throughput of about 37 kbps to 59 kbps is observed. You would expect a throughput of about 1.5 Mbps.

Workaround: There is no workaround. The symptom does not occur in Release 12.3.

IP Routing Protocols

- CSCsb50606

Symptoms: Memory utilization in the “Dead” process grows gradually until the memory is exhausted. The output of the **show memory dead** command shows that many “TCP CBs” re allocated. Analysis shows that these are TCP descriptors for non-existing active BGP connections.

Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.3(13), that has an NPE-G1, and that functions as a PE router with many BGP neighbors. However, the symptom is not platform-specific, nor release-specific.

Workaround: Reload the router. If this is not an option, there is no workaround.

- CSCsc73436

Symptoms: High CPU usage may occur and the table versions of BGP peers are reset to zero.

Conditions: This symptom is observed when you update a complex policy on a Cisco router that has a complex configuration of BGP peers.

Workaround: There is no workaround.

- CSCsc75426

Symptoms: A router that is configured for BGP and that has the **ip policy-list** command enabled may unexpectedly reload because of a bus error or SegV exception.

Conditions: This symptom is observed when BGP attempts to send an update with a “bad” attribute.

Workaround: There is no workaround.

ISO CLNS

- CSCsc63871

Symptoms: When IS-IS and CLNS are configured, a router may enter a state in which only one adjacency is shown in the output of the **show clns interface** command, even though the **show clns neighbors** command may correctly display all the neighbors that are connected to the interface.

When this situation occurs and any one of the neighbors on the segment goes down, all routing updates may be lost. The single adjacency is torn down and despite the fact that the output of the **show clns neighbors** command still shows the neighbors, routing stops because there are no adjacencies.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(18)S1 or Release 12.3(9b) when an adjacency goes down while it is still in the INIT state. The symptom occurs because the adjacency counter is incorrectly decremented. The symptom may also occur in other releases.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface that reports only one adjacency.

Alternate Workaround: Enter the **clear clns neighbors** command on the affected router.

Miscellaneous

- CSCee20451

Symptoms: A VC may experience an output stuck condition.

Conditions: This symptom occurs when using T1 ATM (the IMA function is not used) on a PA-A3-8T1IMA.

Workaround: Perform the **clear interface** command.

- CSCee31719

Symptoms: Multicast packets are not fast-switched on an MDT tunnel interface, causing packets to be blackholed.

Conditions: This symptom is observed on a Cisco router that functions as a PE router in a Multicast VPN environment.

Workaround: There is no workaround.

- CSCeh31441

Symptoms: A line card reloads when traffic is sent through an ATM PVC with the QoS policy enabled.

Conditions: The symptom occurs only with the following configuration.

```
policy-map foo
  class class-default
    shape average <cir>

interface atm1/0/0.
  pvc <vpi>/<vci>
    service-policy output foo
```

Workaround: Add a dummy class to the policy-map with a bandwidth or shape feature as shown in the following example:

```
policy-map foo
  class dummy
    bandwidth <kbps>
  class class-default
    shape average <cir>
```

- CSCeh57734

Symptoms: A router that is configured with redundant RPs that function in RPR+ or SSO mode may generate the following error message after the router has been reloaded:

```
%IPC-2-ONINT: Called from interrupt level: IPC blocking send request
```

After the error message has been generated, the standby RP may reload unexpectedly.

Conditions: This symptom is observed on a Cisco 12000 series that is configured for Multicast VPN and that runs the gsr-p-mz image of Cisco IOS Release 12.0(30)S, Release 12.0(31)S, or an interim release for Release 12.0(32)S.

Workaround: There is no workaround.

- CSCei87255

Symptoms: Traffic does not pass through the main interface of an ATM Engine 2 line card after you have reloaded microcode onto the line card.

Conditions: This symptom is observed on a Cisco 12000 series that runs an interim release for Cisco IOS Release 12.0(32)S. The symptom occurs only for the main interface and not for any subinterfaces. The symptom may also occur on other platforms.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the main interface of the affected ATM line card.

- CSCej33561

Symptoms: Traffic reconvergence times are long after a line card reload.

Conditions: This symptom has been observed on a scaled IP and L3VPN configuration in which E3 cards are installed and part of the data path.

Workaround: There is no workaround.

- CSCej60016

Symptoms: When an SSO switchover occurs less than 10 minutes after the router has been reloaded or a preceding SSO switchover has occurred, the following error message and a traceback are generated:

```
%FIB-4-FIBNULLIDB: Missing idb for fibidb Tunnel0.
```

Configuration: This symptom is observed on a Cisco router that is configured for MVPN.

Workaround: Wait at least 10 minutes after the router has been reloaded or a preceding SSO switchover has occurred before initiating an SSO switchover.

- CSCej83614

Symptoms: Multicast packets are punted to the RP instead of being fast-dropped.

Conditions: This symptom is observed on a Cisco router when an access control list is configured on the egress interface to deny all IP packets.

Workaround: There is no workaround.

- CSCek05730

Symptoms: A Cisco router may crash unexpectedly because of a bus error and/or display some spurious memory accesses.

Conditions: This symptom is observed when an interface that is configured for some form of fancy queueing (that is, anything besides FIFO queueing) actively forwards traffic.

Workaround: Disable fancy queueing on the Ethernet interface.

- CSCek24751

Symptoms: Traffic may not fully recover when you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on an interface that functions as one of two members of a link-bundling port channel.

Conditions: This symptom is observed on a 4-port Gigabit Ethernet ISE line card that is installed in a Cisco 12000 series. The router runs the c12kprp-p-mz image of Cisco IOS Release 12.0(32)S and functions in a scaled configuration with AToM connections that are configured on a link-bundling port channel. The symptom is more likely to occur after the router or line card has just been reloaded.

Workaround: There is no workaround.

- CSCek24997

Symptoms: When you enter the **show diag** command, the output is continuously generated, alternating between the various slots of a line card.

Conditions: This symptom is observed on a Cisco 12000 series.

Workaround: There is no workaround.

- CSCek26835

Symptoms: The **xconnect** command does not function when AToM over MPLS (AToMoMPLS) is configured for VP mode. Although you can enter the **xconnect** command when AToMoMPLS is configured for VP mode, the command is not applied, and the output of the **show running-config** command does not show the Xconnect configuration for the ATM interface.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(32)S. Note that the symptom does not occur when AToMoMPLS is configured for VC mode.

Workaround: Configure AToMoMPLS for VC mode. If this is not an option, there is no workaround.

- CSCek28323

Symptoms: An interface of an Engine 3 ingress line card that functions in feature mode may become stuck, and all traffic may be dropped.

Conditions: This symptom is observed on a Cisco 12000 series that is configured with an Engine 3 ingress line card that has the **hw-module slot slot-number np mode feature** command enabled and that is configured with an egress line card that has a link bundle interface.

Workaround: Disable the **hw-module slot slot-number np mode feature** command on the Engine 3 ingress line card.

- CSCek30152

Symptoms: When a T3/E3 Serial SPA is configured in Kentrox mode with a small bandwidth between 22 kbps and 250 kbps, either in T3 or E3 mode, the firmware miscalculates the bandwidth allocation and allows up to 24M of traffic to pass through.

Conditions: This symptom is observed on a Cisco 7304 and a Cisco 12000 series.

Workaround: Do not configure such a small bandwidth when the T3/E3 Serial SPA is configured in Kentrox mode. The minimal bandwidth on a T3/E3 Serial SPA that is configured in Kentrox mode is either 1500 kbps in T3 mode or 1000 kbps in E3 mode.

- CSCek30377

Symptoms: A SIP may generate an error message or crash when you first perform an OIR of an SPA-10X1GE that is installed in the SIP and you then enter the **show tech-support** command.

Conditions: This symptom is observed on a Cisco 12000 series.

Workaround: There is no workaround.

Further Problem Description: The symptom does not occur when a 1-port OC192/STM64 POS/RPR SPA is installed in the SIP.

- CSCek31439

Symptoms: If the sender and receiver for a multicast group are on the same line card on a PE router, the v flag may be set, causing traffic to be punted to the RP.

Conditions: This symptom is observed on a Cisco 12000 series when a hash collision occurs. The symptom may not be platform-specific.

Workaround: There is no workaround.

- CSCek31489

Symptoms: MQC ingress policing may not filter multicast traffic.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(32)S when the MQC policy map is configured on an OC-12 subinterface of a 1-port channelized OC-48 ISE line card in the ingress direction.

Workaround: There is no workaround.

- CSCek31805

Symptoms: The Total, Switched, and Drops counters in the output of the **show ip mds stats switching** command are merged together (there is no space between the values) when their values become large, preventing you from reading the values.

The merged output looks as follows:

```
11 184467174477999786961844671744778750807211585384 3187420 885240 0
```

The proper output should look as follows:

```
11 18446717447799978696 18446717447787508072 11585384 3187420 885240 0
```

There is no operational impact because the values are correct, just misleading.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S4 and that is configured with multiple Engine 3 and Engine 4+ line cards.

Workaround: There is no workaround.

- CSCek34228

Symptoms: Tracebacks may be generated for a 1-port channelized STM-1/OC-3 SPA that has a multilink configuration. The multilink interface and the 1-port channelized STM-1/OC-3 SPA may not function properly.

Conditions: This symptom is observed when you reload the Cisco 12000 series in which the SPA is installed.

Workaround: There is no workaround.

- CSCek38260

Symptoms: Routers may crash with MPLS VPN configuration and shutting down PE-CE link.

Conditions: The symptoms may occur when the router acts as a PE on the MPLS VPN topology and when one or more PE-CE links are shut down.

Workaround: There are no workaround.

- CSCin95125

Symptoms: dCEF switching does not function when Frame Relay over L2TPv3 is configured on a 2-port OC-3 POS port adapter (PA-POS-2OC3) that is installed in a VIP 6-80.

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(30)S3 when an interface of the PA-POS-2OC3 faces the core of the network. When traffic from the core leaves the PA-POS-2OC3 to a CE router, dCEF switching functions fine. However, when traffic from the CE router leaves the PA-POS-2OC3 to the core, dCEF switching does not function and the VIP 6-80 punts the traffic to the RSP.

Workaround: There is no workaround.

- CSCin97815

Symptoms: Counters in the output of the **show policy-map interface mfr** command do not increment for any type and/or class of service. Even the class default shows no packets. The counters in the output of the **show frame-relay pvc** command show the packets correctly.

Conditions: This symptom is observed when a map class is configured on a subinterface that is part of an MFR (FRF.16) bundle and when the map class consists of both an input and output service policy.

Workaround: There is no workaround.

- CSCsa64457

Symptoms: A router may incorrectly install IPv6 routes that are associated with an ATM interface, even though the ATM interface is down.

Conditions: This symptom is observed when a PVC configuration is applied to the ATM interface.

Workaround: Do not apply a PVC configuration when the ATM interface is down.

- CSCsa65822

Symptoms: Traffic from an Engine 3 or Engine 5 line card to an egress line card that is installed in slot 0 stalls.

Conditions: This symptom is observed on a Cisco 12000 series when you insert a new line card and remove the line card before it reaches the “IOS RUN” state, for example, when the line card is still in the “IOS STRT” or “IOS UP” state.

Workaround: After you have inserted a line card, wait until the line card is in the “IOS RUN” state before you remove it. If the line card becomes stuck before reaching the “IOS RUN” state, remove the line card, and enter the **show controller tofab queue 0** command on other Engine 3 or Engine 5 line cards in the chassis to check if the tofab queues towards slot 0 are uncorrupted. If the queues are corrupted, reload slot 0 to recover from the situation.

- CSCsb00759

Symptoms: A Cisco 3640 or Cisco 3660 stops encrypting GRE packets, which are then sent in the clear.

Conditions: This symptom is observed on a Cisco 3640 and Cisco 3660 that run Cisco IOS Release 12.3(13), that are configured for CEF, and that have an interface (but not the interface with the crypto map) that has that has the **ip tcp header-compression** command enabled and **physical-layer async** command enabled.

Workaround: Enter the **no route-cache cef** command followed by the **route-cache cef** command.

Alternate Workaround: Delete the crypto map from the interface and re-apply the crypto map.

- CSCsb01043

Symptoms: When a Turbo ACL classification table grows beyond a certain size, a memory allocation failure may occur or the router may crash.

If the router runs Cisco IOS Release 12.1E or 12.3, memory corruption may occur, causing the router to crash. If the router runs Cisco IOS Release 12.2S, an error message similar to the following may appear during a Turbo ACL compilation, the compilation will fail, and a recompilation is forced:

```
%SYS-2-CHUNKBADELESIZE: Chunk element size is more than 64k for TACL Block -Process=
"TurboACL", ipl= 0, pid= 82
```

These symptoms do not occur because of an out-of-memory condition.

Conditions: This symptom is observed on a Cisco router that is configured for Turbo ACL. The Cisco 10000 series is not affected.

Workaround: Monitor the output of the **show access-lists compiled** command and force the Turbo ACL tables to be cleared if a table is at risk of growing large enough to trigger the symptoms.

The tables that have significant sizes are the first and third tables shown next to “L1:” and the first table shown next to “L2:”. When the number after the slash for one of these tables is greater than 16384 for the “L1” tables or greater than 32768 for the “L2” table, the table is already too large and the symptom may occur any moment.

When the number is in the range from 10924 to 16384 inclusive for the “L1” tables or the range from 21846 to 32768 inclusive for the “L2” tables, the table size will be too large on the next expansion. An expansion occurs when the number to the left of the slash reaches 90 percent of the value to the right of the slash. When the value to the left of the slash approaches 90 percent of the value to the right, enter the **no access-list compiled** command followed by the **access-list compiled** command to disable and re-enable Turbo ACL. Doing so causes the tables to be cleared and, therefore, delay the expansion. This workaround may be impractical when there is a high rate of incoming packets and when entries are added frequently to the tables.

Alternative Workaround: Disable Turbo ACL by entering the **no access-list compiled** command.

Note that neither of these workarounds are supported on a Cisco 7304 that is configured with an NSE-100: there is no workaround for this platform.

- CSCsb52900

Symptoms: An inconsistency may occur in the outlabel information that is used by BGP and MPLS forwarding.

Conditions: This symptom is observed when there are two route reflectors (RRs) that advertise the same route and when one of the routes is the best path. The symptom occurs when the following conditions are present:

- The PE router that is the source restarts, causing the prefix to be readvertised with a new label.
- The RR that forms the non-best path delays the withdrawal and readvertisement of the prefix, for example, because the RR has a heavy load.

This situation causes BGP to function with the new label but MPLS forwarding to function with the old label.

Workaround: Enter the **clear ip route** *network* command for the affected prefix.

- CSCsb88907

Symptoms: A Cisco 12000 series RP crashes when you enter the **clear l2tun all** command.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(30)S3 when the **debug vpdn l2x-packets** command is enabled on the router.

Workaround: Do not enter the **clear l2tun all** command when the **debug vpdn l2x-packets** command is enabled on the router.

- CSCsc01223

Symptoms: The following symptoms may occur after you have reloaded a router:

- For a session that is in the idle state, the output of the **show l2tun session brief** command may not show a circuit/interface name, that is, the output shows "-".
- Not every session comes up.
- When the **debug ssm cm error** command is enabled, a “Two segs” error is consistently generated in the log.

Conditions: This symptom is observed when multiple L2TPv3 Xconnect links are configured and occurs only after you have reloaded the router.

Workaround: Disable the **xconnect** command for the idle session and then re-enable the same command.

- CSCsc16318

Symptoms: When you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on all serial interfaces of an MLP bundle, a ping fails because OSPF is stuck in the INIT state.

Conditions: This symptom is observed even while the MLP bundle comes up after you have entered the **no shutdown** interface configuration command.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the main interface of the MLP bundle.

- CSCsc30268

Symptoms: When you reload one line card, all other line cards in the chassis may reload unexpectedly.

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(32)S or an earlier release and on a Cisco 7600 series that runs Cisco IOS Release 12.2(18)SX.

Workaround: There is no workaround.

- CSCsc30648

Symptoms: A POS line card that is configured with third-party vendor Small Form-Factor Pluggable Interface Converters (SFPs) and that is installed in a Cisco 12000 series fails the security check.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(30)S3 or Release 12.0(31) during the initial boot process.

Note that when the router runs Release 12.0(28)S3 and you boot the router with the SFPs already installed, the symptom does not occur. However, when you reload the router and then remove and reinsert the SFPs, they do not pass the security check either.

Workaround: There is no workaround.

- CSCsc40236

Symptoms: Incorrect outgoing labels are installed for BGP-IPv4 Multipath prefixes.

Conditions: This symptom has been observed anytime that a label changes from a BGP-IPv4 Multipath peer.

Workaround: Clearing the BGP neighbor should allow the correct labels to be installed.

- CSCsc65393

Symptoms: A 4-port Gigabit Ethernet ISE line card may crash.

Conditions: This symptom is observed on a Cisco 12000 series that is configured for multicast traffic.

Workaround: There is no workaround.

- CSCsc79397

Symptoms: In an MVPN topology running sparse-mode in the core with data-MDTs, an interruption in traffic in the core (e.g. reloading a P router) may cause a PE router to stop sending traffic to the core.

Conditions: The MVPN traffic is riding a sparse-mode data-MDT when a P router is reloaded. The interruption to the traffic causes the traffic to fall back to the default-MDT and the data-MDT sparse group enters the registering state. If the traffic resumes before the data-MDT mroute times out, it will initially be forwarded over the default-MDT and then switch to the data-MDT but no register traffic is sent.

Workaround: Enter the **clear ip mds line x** where x is the Ingress LC on PE router. Note that Cisco recommends the use of SSM for data-MDTs and this will avoid the issue entirely.

- CSCsc82234

Symptoms: A multicast RPF check fails when the **maximum-paths eibgp** command is configured as part of an IPv4 VRF.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(31)S2 and that is configured for L2TPv3.

The symptom occurs because RPF expects the gateway for the VPNv4 route to be either in the same VRF or in the global routing table context, which is not the case when L2TPv3 is configured.

Workaround: Disable the **maximum-paths eibgp** command.

- CSCsc83961

Symptoms: Both the protect and the working APS interfaces receive traffic.

Conditions: This symptom is observed on a Cisco router that is configured with a SIP-600 in which POS SPAs are installed.

Workaround: There is no workaround.

- CSCsc88057

Symptoms: Traffic forwarding stops on the Gigabit Ethernet modular baseboard (EPA-GE/FE-BBRD) of a Modular GbE Engine 4+ line card.

Conditions: This symptom is observed on a Cisco 12000 series when you add an ACL to the 3-port Gigabit Ethernet port adapter (EPA-3GE-SX/LH-LC) of the same Modular GbE Engine 4+ line card.

Workaround: Perform a microcode reload on the 3-port Gigabit Ethernet port adapter of the Modular GbE Engine 4+ line card. Alternately, reload the router. However, note that both workarounds interrupt the traffic flow.

- CSCsc93094

Symptoms: Interface numbering is not complete when executing commands on a Cisco 12000 line card.

Conditions: This symptom has been observed when entering commands on a Cisco 12000 line card which requires multiple physical interfaces on a single controller.

Workaround: There is no workaround.

- CSCsc94359

Symptoms: The BGP table and CEF forwarding table may have mismatched labels for prefixes that are learnt from a remote PE router.

Conditions: This symptom is observed on a Cisco router that functions as a PE router when an eBGP session flap or route flap occurs on the remote PE router. A new label for the prefix is learnt from the remote PE router, but forwarding may not be updated properly.

Workaround: There is no workaround. When the symptom has occurred, and to correct the situation, enter the **clear ip route vrf vrf-name network** command on the PE router that has mismatched labels.

- CSCsc95511

Symptoms: A line card crashes continuously.

Conditions: This symptom is observed when a Cisco router boots with a line card that has an interface on which Frame Relay DLCI, a QoS service policy, and FRF.12 are configured.

Workaround: Ensure that FRF.12 is not configured when the router boots. After the router has booted, add FRF.12.

- CSCsc98510

Symptoms: An enhanced FlexWAN or VIP may reload.

Conditions: This symptom is observed on a Cisco Catalyst 6000 series and Cisco 7600 series (in which a FlexWAN is installed) and on a Cisco 7500 series (in which a VIP is installed). The symptom occurs when these platforms are configured for VRF, MLP, and QoS.

Workaround: There is no workaround.

- CSCsd02602

Symptoms: All channels on a multichannel T3 port adapter may go down. The router may then reload unexpectedly due to a software forced crash. If not, all of the channels in the T3 may stay down until corrective action is taken.

The following messages may appear one or more times in the router or VIP log:

```
%CT3-3-MBOXSENDM: Failed to send msg MBOXP_MSG_T1_DISABLE to bay 1 firmware
```

On a Cisco 7200 router, the following messages may be seen in the log:

```
CT3SW WatchDog not cleared, WatchDog = 2 CT3SW WatchDog not cleared, WatchDog = 3
```

On a Cisco 7500 router, the following messages may be seen in the log:

```
%CT3 5/8: Illegal Love Letter, cmd 0 %CT3 5/9: Illegal Love Letter, cmd 0
```

Conditions: This symptom affects routers using two-port multichannel T3 port adapters, the PA-MC-2T3 and the PA-MC-2T3+. The symptom occurs when one or more of the T1's in either T3 sees framing errors. One-port multichannel T3 port adapters, the PA-MC-T3 and the PA-MC-T3+, are not affected.

Workaround: There is no workaround to prevent this problem. Possible corrective actions are listed below:

Possible Corrective Actions for the Cisco 7200 router:

1. Remove and reinsert the affected port adapter.
2. Simulate removal and reinsertion with these exec mode commands in sequence: **hw-module slot slot-number stop hw-module slot slot-number start**
3. Reload the router.

Possible Corrective Actions for the Cisco 7500 router: 1. Remove and reinsert the VIP with the affected port adapter. 2. Use the configuration mode command: **microcode reload** 3. Reload the router.

- CSCsd02954

Symptoms: Some CEF entries are missing from some VRFs, as shown in the output of the **show ip cef inconsistency now** command.

Conditions: This symptom is observed after an OIR or reload of a Cisco 12000 series GE ISE line card.

Workaround: There is no workaround. When the symptom has occurred, enter the **clear ip cef epoch route vrf** command.

Further Problem Description: So far, the symptom is observed for local "receive" entries, such as /32 entries for a VRF loopback interface. However, the symptom may also occur for other types of VRF FIB entries.

- CSCsd03412

Symptoms: When you load a Cisco IOS software image, the interface-level uRPF configuration may be lost.

Conditions: This symptom is observed on a Cisco 12000 series when the uRPF interface level configuration has the **allow-self ping** keyword enabled in a command such as the **ip verify unicast source reachable-via allow-self-ping** command before you load the Cisco IOS software image.

A list of the affected releases can be found at

<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd03412>. Cisco IOS software releases that are listed under the "All affected versions" link at this location are affected. Cisco IOS software releases that are listed in the "First Fixed-in Version" field at this location are not affected.

Workaround: To prevent the symptom from occurring, remove the **allow-self ping** keyword before you load the Cisco IOS software image. When the symptom has occurred, reconfigure each interface that lost the uRPF configuration and ensure that the **allow-self ping** keyword is not part of a command.

- CSCsd09324

Symptoms: When reloading a router (lsnt-ap-pe1, Cisco 7500 platform) with Cisco IOS interim Release 12.0(31.4)S1 from any Cisco IOS Release 12.0(28)S4b image, several IDBINDEX_SYNC-3-IDBINDEX_ENTRY_LOOKUP and traceback occur in the standby log.

Conditions: This symptom has been observed on a Cisco 7500 router platform with MVPN.

Workaround: There is no workaround.

- CSCsd10973

Symptoms: When an RP switchover occurs after you have reloaded a line card that is configured for MFR and MLP, the MFR and MLP links may remain down.

Conditions: This symptom is observed on Cisco 12000 series that runs Cisco IOS Release 12.0(28)S4, that runs in SSO mode, and that is configured with a 6-port channelized T3 Engine 0 line card and a 1-port channelized OC-12 ISE line card.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected MFR and MLP interfaces.

Further Problem Description: Note that the symptom does not occur when the router runs in RPR+ mode.

- CSCsd11646

Symptoms: On a router that runs Multiprotocol Label Switching (MPLS), the “%SYS-3-OVERRUN:” and “%SYS-6-BLKINFO” error messages may be generated and a software-forced crash may occur on the router.

Conditions: This symptom is observed when you enter the **show mpls ldp discovery** command under the following condition:

- There are multiple LDP adjacencies configured through one interface.
- The adjacencies between peers through this interface have not been fully established for some peers.
- The unestablished LDP adjacencies are coming while you enter the **show mpls ldp discovery** command.

Workaround: Do not enter the **show mpls ldp discovery** command while multiple LDP adjacencies are coming up. Rather, enter the **show mpls ldp neighbor [detail]** command while multiple LDP adjacencies are coming up.

- CSCsd11701

Symptoms: When multicast hardware acceleration is enabled, a wrong label stack may be imposed on packets that have an IP destination address below 16.x.x.x. This situation occurs, for example, when the IP destination address is 10.1.1.1 and when the ingress interface is an MPLS VPN VRF subinterface that is configured for 802.1q. Note that in this situation, the CEF forwarding information is correct, that is, it has the correct label stack.

Conditions: This symptom is observed on a Cisco 12000 series that is configured with a 3-port GRE Engine 2 line card but may occur on any Engine 2 line card that has VRF interfaces. The symptom occurs only when multicast hardware acceleration is enabled.

A list of the affected releases can be found at

<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCei01644>. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

Workaround: There is no workaround.

- CSCsd12941

Symptoms: The CPU usage may remain at 99 percent for a long time when NMS polls the ipRouteTable via the SNMP protocol.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(28)S or Release 12.0(31)S when there is a large number of routes in the routing table.

Workaround: Exclude the ipRouteTable from the SNMP view.
- CSCsd15803

Symptoms: When you enter the **show tech-support cef** or **show cef linecard internal** command, the router may crash.

Conditions: This symptom is observed on a Cisco router that is configured for CEF.

Workaround: There is no workaround.
- CSCsd18361

Symptoms: On a subinterface of a 4-port Gigabit Ethernet ISE line card (4GE-SFP-LC) that has an LDP neighborhood with a neighbor that uses per-interface label space, when the LDP neighborhood goes down, the subinterface stops forward traffic.

Conditions: This symptom is observed on a Cisco 12000 series. The symptom does not occur with a 3-port Gigabit Ethernet line card (3GE-GBIC-SC).

Workaround: There is no workaround.
- CSCsd20210

Symptoms: The PXF engine of a Cisco 10720 may crash.

Conditions: The symptom is observed when you modify an existing access control list (ACL) that is attached to an interface.

Workaround: Do not modify an ACL that is attached to an interface. If you cannot remove the ACL from the interface, create a new ACL and apply it to the interface.
- CSCsd23189

Symptoms: The **ip helper-address** command does not function on a 4-port Gigabit Ethernet ISE line card (4GE-SFP-LC).

Conditions: This symptom is observed on a Cisco 12000 series when the Gigabit Ethernet interface is configured for VRF forwarding.

Workaround: There is no workaround.
- CSCsd24601

Symptoms: The FIB becomes disabled when you bring down a member link of an MLP or MFR bundle.

Conditions: This symptom is observed on a Cisco 7500 series that is configured with an MLP or MFR bundle and that runs Cisco IOS Release 12.0(30)S, Release 12.0(31)S, or Release 12.0(32)S, all of which integrate the fix for caveat CSCeg57219. Other Cisco IOS software releases that integrate the fix for caveat CSCeg57219 are not affected.

Workaround: There is no workaround.
- CSCsd26348

Symptoms: An ISE line card crashes when the MPLS VPN-VRF Selection Based on Source IP Address feature is enabled.

Conditions: This symptom is observed on a Cisco 12000 series when the MPLS VPN-VRF Selection Based on Source IP Address feature is enabled in the configuration.

Workaround: Do not enable the MPLS VPN-VRF Selection Based on Source IP Address feature.

- CSCsd28415

Symptoms: When only one T1 link in a MLP bundle is active while all other links are shut down, the bundle does not pass traffic unless you bring up at least one more T1 link in the bundle.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S2.

Workaround: Bring up a second T1 link in the MLP bundle.

- CSCsd30704

Symptoms: When you first enter the **router isis area-tag** command followed by the **address-family ipv6** command and then change the administrative distance for the address-family IPv6 configuration, the RP may crash.

Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of Cisco IOS Release 12.0(30)S5, Release 12.0(31)S3, or Release 12.0(32)S1. The symptom may also occur on other platforms.

Workaround: There is no workaround.

- CSCsd34318

Symptoms: The output of the **show memory bigger** command shows negative block sizes for 4 GB of RAM.

Conditions: This symptom is observed on a Cisco 12000 series when a block with a size greater than 2 GB is also present.

Workaround: There is no workaround.

- CSCsd34463

Symptoms: An Engine 4, Engine 4 plus, or Engine 6 line card may punt MPLS packets to the RP, causing the CPU usage of the RP to be high.

Conditions: This symptom is observed on a Cisco 12000 series that receives a large number of small MPLS packets that have their TTL set to 1.

Workaround: There is no workaround.

- CSCsd35405

Symptoms: A line card that is configured with a multilink bundle may reset when the connected serial T1 interface on the remote router is shut down while traffic is flowing.

Conditions: This symptom is observed on a Cisco 12000 series when the traffic that enters the multilink bundle exits over an L2TPv3 tunnel and when multilink fragmentation is applied at the remote end.

Workaround: Disable multilink fragmentation at the remote end. If this is not an option, there is no workaround.

- CSCsd36528

Symptoms: In an MVPN topology, an Engine 5-based SIP (that is, a SIP-401, SIP-501, SIP-600, or SIP-601) in which one or more SPAs are installed may reset when you forward multicast traffic with packets that are larger than the MTU of the interface and therefore require fragmentation.

Conditions: This symptom is observed on a Cisco 12000 series, that functions as a PE router, and that is located in the network core when a SPA that is installed in the SIP interconnects the PE router with a P router.

Workaround: There is no workaround.

- CSCsd37840

Symptoms: When a Cisco 7500 series that runs in SSO mode reloads (for example, because of a “c7500 CCB PLAYBACK” error), the active RP comes up properly but the standby RP crashes. When the router reloads while running in RPR+ mode, the standby RP does not crash but an “%HA-3-SYNC_ERROR: CCB Playback error” message is generated.

Conditions: This symptom is observed on a Cisco 7500 series that is configured for SSO or RPR+.

Workaround: There is no workaround. The symptom does not occur when you disable SSO or RPR+.

- CSCsd38657

Symptoms: An RP crashes when a Gigabit Ethernet interface of a SPA is shut down. When this situation occurs, the following error message and traceback is generated:

```
Unexpected exception to CPUvector 700, PC = 2CEE34 -Traceback= 2CEE34 4C40000 2D8958
2D8D2C 2C1164 14048C 2CFB4C
```

If a crashinfo file is generated, the last log message is the following:

```
%SYS-6-STACKLOW: Stack for process CEF process running low, 0/6000
```

On a router that is configured with two RPs that function in RPR+ mode, when the RP crashes, a switchover occurs. However, the crashed RP does not come up and remains in standby mode.

Conditions: These symptoms are observed on a Cisco router when the recursive lookup on a static MPLS route does not specify a next hop interface. For example, the symptom occurs when the **ip route destination-prefix mask next-hop1** command is enabled but does not occur when the **ip route destination-prefix mask interface1 next-hop1** command is enabled.

Workaround: Ensure that the *interface* argument is included in the static route, as in the following command: **ip route destination-prefix mask interface1 next-hop1**.

- CSCsd40253

Symptoms: Aggregated Output NetFlow may aggregate output traffic on an incorrect prefix (such as 0.0.0.0/0) on a PE router that functions in an MPLS VPN environment.

Conditions: This symptom is observed on a SIP-600 that is installed in a Cisco 12000 series that runs Cisco IOS Release 12.0(32)S when egress traffic streams are sent in different routing contexts (via the global routing table and via a VRF or different VRFs) and when Aggregated Output NetFlow is enabled using a Prefix-ToS aggregation scheme.

The symptom occurs for both IP-to-IP and tag-to-IP traffic (the latter one from the MPLS core). The symptom does not occur when the egress traffic is within the same routing context, that is, when all egress interfaces are either in the global routing table or in the same VRF).

Workaround: There is no workaround.

- CSCsd43102

Symptoms: On a GSR router configured for MVPN, the reload of any E3 Edge facing line card can cause VRF mroutes to be missing on the reloaded line card while they are present on PRP and on other line cards. This will cause punts to PRP CPU and, depending on number of missing mroutes, potentially high PRP CPU utilization due to IP Input.

Conditions: This symptom has been observed to happen in a scaled MVPN environment and is triggered only by linecard reload.

Workaround: There is no workaround. To recover from this state, issue **clear ip mds linecard linecard-slot- number** where *linecard-slot-number* is the slot number of the reloaded line card.

- CSCsd45263

Symptoms: A router may crash when you unconfigure an MLP bundle that is configured for QoS.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(32)S when the MLP bundle is configured on a 1-port channelized OC-12 ISE line card.

Workaround: There is no workaround.

- CSCsd46458

Symptoms: When you reload a 2-port clear channel T3/E3 Engine SPA that is installed in a PE router that performs MVPN encapsulation, multicast traffic does not resume.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(32)S1 and that functions as a PE router in an MVPN topology.

Workaround: Enter the **ip mds linecard linecard-slot-number *** command. For the *linecard-slot-number* argument, enter the SIP and the slot number in which the SIP is installed.

- CSCsd47404

Symptoms: When configuring output ACL in an interface of an E4+ EPA-GE/FE-BBRD card, the following error message is shown. However, the output of **show tcam-mgr gen7 appl acl-out block-info** shows that there are 964 free entries in TCAM.

```
SLOT 9:Feb 23 00:07:54: %FM-3-TCAM_FAIL: Write label: 0, direction:
egress to TCAM error:
failed to program all entries (partly programmed). Performance will be
seriously degraded for traffic hitting ACL rules beyond hardware capability.
-Process= "Feature Manager", ipl= 0, pid= 46 -Traceback= 40030CBC
404EB828 404EB419C 404E4784 SLOT 9:Feb 23 00:08:01: %FM-3-TCAM_FAIL:
Write label: 0,
direction: egress to TCAM error:
failed to program all entries (partly programmed). Performance will be
seriously degraded for traffic hitting ACL rules beyond hardware capability.
-Process= "Feature Manager", ipl= 0, pid= 46 -Traceback= 40030CBC
```

Conditions: This symptom has been observed in an E4+ LC card when the line card does not find enough free sequential entries in TCAM at its current location because of ACL expansion and needs to relocate ACL to a different location within the TCAM.

Workaround: Perform a workaround similar to the example which follows:

An example configuration of **access-list 102** and **103** applied on GigabitEthernet interface at 9/0/1.

1. Remove all of the ACL applied to that line card interfaces globally. **config terminal no access-list number** [*number* = 102, 103]
2. Remove all of the ACL configuration from the line card interfaces. **config terminal interface GigabitEthernet 9/0/1 no ip access-group number out** [*number* = 102, 103]
3. On line card confirm that the ACLs have been removed. **show access-lists gen7-fm label**
4. Recreate the ACL globally, which are the ACL deleted in Step 1.
5. Re-apply the ACL configuration to the LC interfaces, the one's deleted in Step 2.
6. On the line card, confirm that the ACLs have been recreated properly. **show access-lists gen7-fm label**

- CSCsd49374

Symptoms: When you reload a channelized T3 SPA that is installed in a PE router, all interfaces on a directly-connected channelized T3 SPA that is installed in a CE router remain in the down state, and the following error message is generated:

```
%SPA_CHOC_DSX-3-SPA_CMD_SEND_ERR: Failed to send ipc_send_rpc_blocked command to SPA
```

Conditions: This symptom is observed in a VPN topology on a Cisco 12000 series that runs Cisco IOS Release 12.0(32)S1, that functions as a PE router, and that is connected to another Cisco 12000 series that functions as a CE router. The channelized T3 SPA in the PE router is installed in a SIP-601; the channelized T3 SPA in the CE router is installed in a SIP-400.

Workaround: Reload the channelized T3 SPA in the CE router.

- CSCsd50379

Symptoms: A 12000 series may indicate a low I/O memory condition. The output of the **show memory summary** command shows the following:

Head	Total (b)	Used (b)	Free (b)	Lowest (b)	Largest (b)	
Processor	6101020	3553619936	72555296	3481064640	3472164032	2093048
I/O	DBE00000	33554432	33554232	200	200	156
PCI	D9E00000	33554432	33401688	152744	152744	152700
Fast	60E1020	131072	130008	1064	1064	1020

Conditions: This symptom is observed on a 12000 series that is configured with a PRP2 and 4 GB of RAM.

Workaround: There is no workaround.

- CSCsd54920

Symptoms: An Engine 3 line card may crash with the following message:

```
SLOT 9:Mar 2 21:44:31.827 PST: %SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = MDFS LC Process.
```

Conditions: This symptom has been observed when a large number of mroutes (20K) and egress multicast QoS are configured. The symptom can be triggered by removing and adding the **ip multicast-routing distributed** command.

Workaround: There is no workaround.

- CSCsd58355

Symptoms: The system cannot recover from an RPR+ Switchover.

Conditions: The symptom has been observed in a system scale testbed with both L3VPN and MVPN scaled configurations with the following:

- 4 active E3 Edge line cards
- 907 eBGP sessions
- 1190 L3VPN interfaces
- 214k VPNv4 routes
- 15k multicast routes

Workaround: A possible recovery is to use proc-max-time of 20 msec. This recovery works with E4P and E5 as the Core facing line cards.

- CSCsd62272

Symptoms: The ip2tag unicast traffic from an E3 line card to an E3 line card is being dropped on a GSR.

Conditions: This symptom has been observed on a GSR running Cisco IOS Release 12.0(32)S 060307 nightly image where the GSR is acting as a PE router. The router is configured with unicast VPN and multicast VPN and unicast and multicast traffic is flowing through the router.

Workaround: There is no workaround.

- CSCsd73063

Symptoms: After removing VRF, the following message with tracebacks is observed:

```
%GENERAL-3-EREVENT, %ALIGN-3-SPURIOUS, and %ALIGN-3-TRACE
```

Conditions: This symptom has been observed on a Cisco 12000 router with Cisco IOS Release 12.0(32)S.

Workaround: There is no workaround.

- CSCsd75890

Symptoms: On a bulk sync (reload) of a standby route processor (RP) or during an initial router reload, all MDT configuration is erased on the standby. This erasure causes all MVPN traffic to fail following an RP switchover.

Conditions: This symptom occurs on a dual RP router in RPR+ or SSO mode with MVPN configuration. This symptom is only seen in conn_isp and the Cisco IOS Release 12.0(32)S throttle branch.

Workaround: Deconfigure and reconfigure **mdt default** and **mdt data** configuration statements within the VRF configuration.

Further Problem Description: This symptom occurs as a result of a bug in the initial CSCsd09324 commit.

- CSCsd77990

Symptoms: Under some Cisco 12000 router configurations after a line card reload of a 4GE ISE line card or RPR+ switchover, some interfaces on a 4GE ISE line card can stop receiving traffic.

Conditions: This symptom has been observed on a Cisco 12000 router with Cisco IOS Release 12.0(32)S.

Workaround: There is no workaround. Using the **shutdown** and **no shutdown** commands on the main interface recovers from this symptom.

- CSCsd82249

Symptoms: In MPLS VPN topology, where E3 4xOC12 ATM line card is a Core-facing line card, after performing a reload on any of Egress line cards, the ATM line card may reload.

Conditions: This symptom has been observed on a E3 4xOC12 ATM line card configured with MPLS Aware Netflow, on a Cisco 12000 series that runs Cisco IOS Release 12.0(32)S2 or 12.0(32.1)S4.

Workaround: There is no workaround.

- CSCsd88944

Symptoms: Decapsulation traffic stops forwarding if traffic for the encapsulation stream is stopped when MVPN traffic is flowing bi-directionally on a PE router and the two streams collide with each other and the encapsulation stream occupies the hardware hash table entry.

Conditions: This symptom has been observed when sending MVPN traffic in both directions on an E3 line card, ensuring that one stream collides with the other stream.

Workaround: Use the **clear ip mroute [vrf vrf-name] [* | group [source]]** to clear this issue.

Wide-Area Networking

- CSCsd06510

Symptoms: Unexpected drops may occur in the Multilink Frame Relay (MFR) output hold queue. The drops persist under a very low (25 pps) transmit rate.

The MFR output hold queue may become congested, causing all traffic to fail.

After you have disabled the traffic source or shut down the ingress interface, the MFR output hold queue may take as long as 15 minutes to “drain.”

Conditions: These symptoms are observed on a Cisco router when you run multicast traffic over GRE tunnel interfaces that in turn use an MFR interface for transport.

Workaround: Disable multicast fast-switching.

- CSCsd21476

Symptoms: A router crashes when you attempt to delete a Frame Relay-to-Ethernet connection.

Conditions: This symptom is observed when you first remove the Frame Relay interface via an OIR and then you attempt to delete the Frame Relay-to-Ethernet connection.

Workaround: Re-insert the Frame Relay interface before attempt to delete the Frame Relay-to-Ethernet connection.

Resolved Caveats—Cisco IOS Release 12.0(32)S1

Cisco IOS Release 12.0(32)S1 is a rebuild of Cisco IOS Release 12.0(32)S. The caveats listed in this section are resolved in Cisco IOS Release 12.0(32)S1 but may be open in previous Cisco IOS releases. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCek24204

Symptoms: Multicast traffic stops leaving from a SPA that is installed in a SIP-400 after an RPR+ switchover is performed on the remote end.

Conditions: This symptom is observed on a Cisco 12000 series when the remote end is also a Cisco 12000 series in which a SIP-400 is installed.

Workaround: Enter the **clear ip mds linecard** *linecard-slot-number* command on the SIP-400 that is installed in the local Cisco 12000 series. Note that the *linecard-slot-number* argument represents the SPA and affected output port.

- CSCsb78504

Symptoms: When you enter the **clear cef linecard** command on a SIP-400 or SIP-600 in which channelized T1 and T3 SPAs are installed that are configured with MFR and MLP interfaces, the MFR interfaces may flap. The symptom may also occur when a line card that has MFR and MLP interfaces configured is reloaded or when the router is reloaded.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(32)S, that functions as a PE router, and that has multilink interfaces configured. The symptom is reproducible when CPU-intensive applications are running on the router while a large number of multilink interfaces is brought up. Note that the symptom does not occur for non-SPA line cards.

Workaround: Shut down the multilink interfaces. When the router is stable (that is, after CEF is cleared or after the line or router is reloaded), bring up the multilink interfaces.

Alternate Workaround: Increase the bundle link parameters on the PE router and the connected CE router by increasing the hello and acknowledgement periods via the *seconds* arguments in the following commands for each of the serial interfaces that are part of the multilink bundle:

- **frame-relay multilink hello** *seconds*
- **frame-relay multilink ack** *seconds*

- CSCsc56944

Symptoms: After you have configured VPN, when the default MTU on an interface of an Engine 5 SPA is changed, the Engine 5 SPA may generate tracebacks.

Conditions: This symptom is observed on a Cisco 12000 series that has a VPN configuration when the MTU is changed while traffic is flowing.

Workaround: Do not change the default MTU size on an Engine 5 SPA.

- CSCsc93277

Symptoms: MFR interfaces that are configured on T1 and T3 SPAs that are installed in a SIP-601 may remain in the IDLE state.

Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of Cisco IOS Release 12.0(32)S when any action occurs that changes the MFR link state followed by an RPR+ switchover.

The actions that change the MFR link state include the following:

- Entering the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on an MFR interface.
- Performing a microcode reload of SIP in which the SPAs are installed.
- Entering the **hw-module slot slot-number shutdown** command followed the **no hw-module slot slot-number shutdown** command on the SIP in which the SPAs are installed.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on affected MFR interface.

- CSCsd09718

Symptoms: Packet loss may occur for approximately 200 ms on an Engine 5 SPA.

Conditions: This symptom is observed on a Cisco 12000 series when a standby Route Processor (RP) is inserted or removed.

Workaround: There is no workaround.

- CSCsd28013

Symptoms: Traffic does not pass on some MFR interfaces after an RPR+ switchover has occurred.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(32)S.

Workaround: Reload the SIP (and consequently the SPA) to enable all serial interfaces to enter the up/up state.

Wide-Area Networking

- CSCsd11874

Symptoms: When you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on an MFR interface when the bundle links are down, the serial interfaces that are associated with the MFR interface remain in the IDLE state.

Conditions: This symptom is observed on a Cisco router that is configured for MFR.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on each serial interface that is associated with the MFR interface.

Resolved Caveats—Cisco IOS Release 12.0(32)S

All the caveats listed in this section are resolved in Cisco IOS Release 12.0(32)S. This section describes only severity 1, severity 2, and select severity 3 caveats.

Basic System Services

- CSCdu32036

Symptoms: When you attempt to apply an access list for SNMP by entering the **snmp-server tftp-server-list** command, the access list is not applied. This situation makes it possible to copy the configuration to and from any server, regardless of the contents of the access list.

Conditions: This symptom is observed on a Cisco platform that is configured for SNMP.

The following sample configuration causes the platform to reject configuration file transfers via SNMP from all hosts except the TFTP server that is specified in access list 5:

```
snmp-server tftp-server-list 5
access-list 5 permit 10.1.1.1
snmp-server community private RW 5
snmp-server tftp-server-list 5
```

Workaround: Apply a more general access list to restrict traffic to and from the affected platform.

Alternate Workaround: Disable the SNMP.

- CSCea56560

Symptoms: Configuring nonexistent NTP peers repeatedly may cause a router or switch to reload unexpectedly.

Conditions: This symptom is observed on a Cisco router and Cisco switch that are configured for NTP.

Workaround: Do not add and delete nonexistent NTP peers in quick succession, for example by using a cut-and-paste operation.

- CSCec75641

Symptoms: A Cisco router may reload when there are two or more Telnet or console sessions to the router.

Conditions: This symptom is observed when the following events occurs:

- In one session, enter the **show ip as-path-access-list *acl-number*** command. The output pauses at the “--more--” prompt when there is more than one page output.
- In another session, enter the **no ip as-path access-list *acl-number*** command in which the *acl-number* argument is the same one as in the **show ip as-path-access-list *acl-number*** command.
- In the first session, type in “enter” or “space” in the first session to display the rest of the show command output.

Workaround: Do not enter the **show ip as-path-access-list *acl-number*** command when the **no ip as-path access-list *acl-number*** command is being configured.

- CSCed44414

Symptoms: When the slave RSP crashes, a QAERROR is observed in the master console, resulting in a cbus complex. The cbus complex will reload all the VIPs in the router.

Conditions: This symptom happens when the slave crashes in a period when there is a large number of packets going towards the RSP. A large number of packets go to the RSP when CEF switching is configured or when routing protocol updates are numerous.

Workaround: There is no workaround.

- CSCeh47604

Symptoms: An OER border component does not sent passive updates for OER prefixes, preventing the prefixes from being controlled. The prefixes cycle from the default state to the hold-down state back to the default state.

Conditions: This symptom is observed when NetFlow is configured and when the mode monitor is configured to be “passive” or “both”.

Workaround: Configure the mode monitor to be “active”. The functionality of the mode monitor is limited to the “active” mode only.

- CSCeh71577

Symptoms: A Cisco 7200 series does not load an image and generates a traceback.

Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.4(1), that is configured with an NPE, and that has the L3 cache disabled. The symptom may also occur in other releases.

Workaround: Enable the L3 cache by entering the **no l3 cache disable** command.

- CSCeh85083

Symptoms: A router crashes when you remove a port channel.

Conditions: This symptom is observed under rare circumstances on a Cisco router that is configured for Cisco Discovery Protocol (CDP) and that has hundreds of subinterfaces when you enter the **no interface port** command followed by the **interface port** command.

Workaround: After you have entered the **no interface port** command, wait a few seconds before you enter the **interface port** command.

Alternate Workaround: Disable CDP.

- CSCei77083

Symptoms: A spurious memory access may be generated on an RSP when a VIP that is in a disabled or wedged condition is recovered because of a Cbus Complex or microcode reload.

Conditions: This symptom is observed on a Cisco 7500 series that has a VIP that is in a disabled or wedged condition after the router has booted.

Workaround: There is no workaround.

- CSCej08355

Symptoms: The active Supervisor Engine or Route processor (RP) may reload when the standby Supervisor Engine or RP is inserted.

Conditions: This symptom is observed on a Cisco switch or router when the following conditions are present:

- The SSO redundancy mode is configured.
- The **snmp mib notification-log default** command is enabled.

Workaround: Do not configure SSO as the redundancy mode. Rather, configure RPR+ as the redundancy mode.

Alternate Workaround: Disable the SNMP MIB notification log by entering the **no snmp mib notification-log default** command.

- CSCsa92394

Symptoms: A router may crash while loading the image for a secondary RSP from a disk during the boot process.

Conditions: This symptom is observed on a Cisco 7500 series that is configured with redundant RSPs when the **hw-module slot slot-number image disk0: image** command is configured.

Workaround: There is no workaround.

- CSCsa98777

Symptoms: An MSFC may reload when the standby Supervisor Engine 720 is inserted. Similarly, the active Route Processor (RP) may reload when the standby RP is inserted.

Conditions: These symptoms are observed on a Cisco Catalyst switch or router when SNMP and SSO are configured, and when the following configuration is present on the platform:

```
snmp mib notification-log default
snmp mib notification-log globalageout 600
snmp mib notification-log globalsize 1500
```

Workaround: Do not configure SSO. Rather, configure RPR+.

Alternate Workaround: Remove the SNMP MIB notification-log configuration by entering the **no snmp notification-log default** command.

- CSCsb08386

Symptoms: A router crashes when you enter the **show ip bgp regexp** command.

Conditions: This symptom is observed on a Cisco router when BGP is being updated.

Workaround: Enable the new deterministic regular expression engine by entering the **bgp regexp deterministic** command and then enter the **show ip regexp** command. Note that enabling the new deterministic regular expression engine may impact the performance speed of the router.

- CSCsb14026

Symptoms: A standby RSP reloads continuously.

Conditions: This symptom is observed on a Cisco 7500 series that is configured for SSO and that has the **snmp mib notification-log default** command enabled.

Workaround: Disable the **snmp mib notification-log default** command.

- CSCsb14371

Symptoms: A Cisco 7500 series may log the following error message even if no VIP is installed in slot 0:

```
%IPC_RSP_CBUS-3-NOHWQ: Hardware queue for card at slot 0 not found
```

Conditions: This symptom is observed after a crash of another VIP has occurred. Sometimes the symptom occurs when a VIP is installed in slot 0 but most of the time there is no VIP in slot 0 when the symptom occurs.

Workaround: There is no workaround.

- CSCsb44308

Symptoms: A Cisco router or switch may crash when you enter the **no snmp-server** command.

Conditions: This symptom is observed after a switchover when you enter the **no snmp-server** command on the newly active RP or Supervisor Engine.

Workaround: There is no workaround.

- CSCsb98906

Symptoms: A memory leak may occur in the “BGP Router” process.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(26)S6, that is configured for BGP, and that has the **bgp regexp deterministic** command enabled.

Workaround: Disable the **bgp regexp deterministic** command.

IBM Connectivity

- CSCeg10448

Symptoms: DLSW transparent redundancy does not function via a Fast Ethernet port adapter.

Conditions: This symptom is observed when you use a Fast Ethernet port adapter with a particular third-party vendor chipset.

Workaround: Use a port adapter that uses a different chipset.

Interfaces and Bridging

- CSCee22523

Symptoms: A VIP that contains a PA-A3-OC12 ATM port adapter may unexpectedly reload.

Conditions: This symptom is observed on a Cisco 7500 series that functions in an ATM LANE configuration.

Workaround: There is no workaround. The traffic on the VIP is disrupted until the VIP comes back up.

- CSCef01220

Symptoms: A Versatile Interface Processors (VIP) with a PA-MC-8TE1 port adapter may report its memory size as unknown even though the VIP appears to function normally, and Distributed Multicast Fast Switching (DMFS) may fail to function properly.

Conditions: This symptom is observed on a Cisco 7500 series when any of the following conditions are present:

- The mode of the controller of the PA-MC-8TE1 port adapter is not set to T1 or E1 and you insert or remove another VIP with any port adapter via an OIR.
- Irrespective of whether or not the mode of the controller of the PA-MC-8TE1 port adapter is set to T1 or E1, you insert or remove a standby RSP via an OIR.

Workaround: Enter the **card type {t1 | e1} slot [bay]** command on the PA-MC-8TE1+ port adapter and ensure that none of the controllers on this port adapter are shut down.

- CSCef49896

Symptoms: Packets that enter an interface that is configured for IP may not be switched via dCEF.

Conditions: This symptom is observed on a Cisco 7500 series.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface.

ALternate Workaround: If many interfaces are affected, reload all port adapters by entering the **microcode reload** command on the control plane of the RSP.

- CSCef82084

Symptoms: Spurious memory accesses occur on a Cisco 7200 series and ALIGN-3-SPURIOUS error messages are generated.

Conditions: This symptom is observed after you have configured a new MLP interface and a new EBGp neighbor.

Workaround: There is no workaround.

- CSCeh10624

Symptoms: A Cisco 7206VXR may reload unexpectedly because of a bus error.

Conditions: This symptom is observed on a Cisco 7206VXR that runs Cisco IOS Release 12.3(10a) and that is configured with an NPE-G1 and a couple of PA-MC-8TE1+ port adapters. The symptom may also occur in other releases.

Workaround: There is no workaround.

- CSCeh43864

Symptoms: The line protocol on the POS interface of a PA-POS-OC3 port adapter flaps continuously.

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS interim Release 12.3(14.10) but may also occur in other releases.

Workaround: There is no workaround.

- CSCei25164

Symptoms: A Cisco 7xxx series router may crash because of a bus error exception and may report CPUHOG message when you perform an OIR of an ATM PA-A3 or ATM PA-A6 port adapter.

Conditions: This symptom is observed on a Cisco 7xxx series router that runs Cisco IOS Release 12.3 when PVC auto-provisioning is enabled on the ATM PA-A3 or ATM PA-A6 port adapter and when many PPP sessions are in transition. The symptom may also occur in other releases.

Workaround: There is no workaround.

- CSCei68284

Symptoms: POS interfaces may remain in the up/down state after the router has been reloaded.

Conditions: This symptom is observed on a Cisco Catalyst 6500 series, Cisco 7500 series, and Cisco 7600 series.

Workaround: Reload the FlexWAN or VIP in which the POS port adapter is installed.

- CSCin67809

Symptoms: CEF, dCEF, and fast-switching counters are not accurate on outbound serial E1 or T1 interfaces.

Conditions: This symptom is observed on a Cisco 7200 series when CEF, dCEF, and fast-switching are enabled on a serial E1 or T1 interface.

Workaround: There is no workaround.

- CSCin75573

Symptoms: When you perform an OIR of a PA-MC-8TE1+ or PA-MC-8E1 port adapter, the following error message and traceback may be generated:

```
%ALIGN-3-SPURIOUS: Spurious memory access made at 0x60379D34 reading 0xD8 %
ALIGN-3-TRACE: -Traceback= 60379D34 604F1CFC 60BD0664 6032B93C 6039A0CC 6010A908
6032AA7C 6032EBAC
```

Conditions: This symptom is observed on a Cisco router when the port adapter is configured for QOS on an egress serial interface and traffic is flowing through this interface.

Workaround: There is no workaround.

- CSCin88976

Symptoms: AToM Xconnect does not function.

Conditions: This symptom is observed when L2 switching is configured.

Workaround: There is no workaround.

- CSCsa46510

Symptoms: When you enter the **microcode reload** command, an error message similar to the following and a traceback may be generated:

```
RSP-3-RESTART: interface Serial3/0/1/4:0, not transmitting
-Traceback= 404436B4 4044DE10
```

Conditions: This symptom is observed on a Cisco 7500 that is configured with an E1, T1, E3, or T3 port adapter.

Workaround: There is no workaround.

- CSCsa83897

Symptoms: A channelized T3 port adapter cannot detect C-bit errors and does not shut down after continuous C-bit errors.

Conditions: This symptom is observed on a Cisco 7200 series that is configured with a channelized T3 port adapter.

Workaround: There is no workaround.

- CSCsa87986

Symptoms: A router may intermittently transmit corrupt PPP packets. When you enter the **debug ppp nego** and **debug ppp errors** commands, it appears that “protocol reject” packets are received from the remote end.

Conditions: This symptom is observed on a Cisco 7500 series that has only one OC-3 POS port adaptor per VIP and that is configured for PPP encapsulation.

Workaround: Configure an outbound policy on the interfaces of the OC-3 POS port adaptors.

- CSCsb04481

Symptoms: CEF may fail and the following error message is generated:

```
Interface Serial0/0:63 changed state to down %CT3-3-LOVEFAIL: CT3-SW-PA-0/0: failed
to send T3 line state change love letter %AMDP2_FE-5-LATECOLL: Ethernet0/0 transmit
error
```

Conditions: This symptom is observed on a Cisco 7500 series that is configured with a channelized T3 port adapter.

Workaround: There is no workaround.

- CSCsb51879

Symptoms: A Cisco 7500 series may generate the following error message and traceback:

```
%IPC-2-ONINT: Invalid operation at interrupt level: IPC blocking send request 103000C
-Traceback= 40857C4C 40291754 40291AC4 40295214 4028BD1C 4028BBA0 4026C5A8 4075FF30
407615F0
```

Conditions: This symptom is observed on a Cisco 7500 series that is configured with a PA-MC-xT1/E1 type of port adapter.

Workaround: There is no workaround.

- CSCsb65340

Symptoms: An interface may not be able to receive OSPF hello packets.

Conditions: This symptom is observed after you have entered the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the peer interface, causing a link up/down event to occur.

Workaround: Reconfigure OSPF.

Further Problem Description: The symptom occurs because the address filter entry is deleted during the link up/down event. You can verify that the symptom has occurred in the output of the **show controller** command and you can manually confirm the deletion of the OSPF MAC entry. When you reconfigure OSPF, the OSPF MAC entry is re-inserted in the address filter.

- CSCsc17534

Symptoms: Unicast packets are not CEF-switched on a VIP but are fast-switched on the RP.

Conditions: This symptom is observed on a Cisco router that has a VIP only when the ingress interface is an ISL subinterface.

Workaround: There is no workaround.

- CSCsc29478

Symptoms: Interfaces of a serial port adapter fail and do not come into service, preventing you from establishing links or tunnels via these interfaces.

Conditions: This symptom is observed on a Cisco 7500 series that runs an interim release for Cisco IOS Release 12.0(32)S.

Workaround: There is no workaround.

IP Routing Protocols

- CSCdz84521

Symptoms: Selective Packet Discard (SPD) with an IP precedence of 6 and 7 may not function correctly. Packets may be treated as nonpriority packets. SPD is used when a queue is filling (for example, because of a flap or change) and routing traffic must be guaranteed a high priority and not dropped while the interface recovers. In this situation, routing traffic with an IP precedence of 6 and 7 is not given proper priority, and the recovery process may be delayed.

Conditions: This symptom is observed with incoming traffic on any interface of a Cisco 7200 series and may be observed on other Cisco platforms as well.

Workaround: There is no workaround.

- CSCec12299

Devices running Cisco IOS versions 12.0S, 12.2, 12.3 or 12.4 and configured for Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) or VPN Routing and Forwarding Lite (VRF Lite) and using Border Gateway Protocol (BGP) between Customer Edge (CE) and Provider Edge (PE) devices may permit information to propagate between VPNs.

Workarounds are available to help mitigate this vulnerability.

This issue is triggered by a logic error when processing extended communities on the PE device.

This issue cannot be deterministically exploited by an attacker.

Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080924-vpn.shtml>.

- CSCec23167

Symptoms: During BGP scalability testing, error messages and tracebacks similar to the following ones may be logged, indicating a difficulty with TCP and buffer usage:

```
%SYS-2-MALLOCFAIL: Memory allocation of 4692 bytes failed from 0x6076F714, align
Pool: I/O Free: 11143248 Cause: Memory fragmentation
Alternate Pool: None Free: 0 Cause: No Alternate pool
-Process= "Pool Manager", ipl= 0, pid= 6
-Traceback= 607FE10C 607FF1EC 6076F71C 6080C1D0 6080C400

%TCP-6-NOBUFF: TTY0, no buffer available
-Process= "BGP I/O", ipl= 0, pid= 139
-Traceback= 6098B4EC 609938C8 60993C1C 60D55CE4 60D0BEB0

%TCP-6-NOBUFF: TTY0, no buffer available
-Process= "BGP Router", ipl= 0, pid= 138
-Traceback= 6098B4EC 609938C8 60993C1C 60D55CE4 60D29858 60D2AF88 60D1B4BC
```

Conditions: This symptom is observed on a Cisco router that is in the processing of building BGP sessions for about 80,000 prefixes and about 1200 BGP peers.

Workaround: There is no workaround.

- CSCed50220

Symptoms: The RP and SP MFIB tables are not synchronized, preventing the outgoing interfaces for multicast flows from matching.

Conditions: This symptom is observed when you reload a Cisco Catalyst 6000 series or Cisco 7600 series that are configured for multicast. The symptom may be platform-independent.

Workaround: There is no workaround.

- CSCef21601

Symptoms: Calls may not complete because ResvConfirm messages are dropped. You can enter the **debug ip rsvp messages** command to track RSVP messages as they traverse routers.

Conditions: This symptom is observed when RSVP is configured for call admission control in a network with routers that do not have RSVP and a proxy ARP enabled. The symptom occurs because the RSVP-capable hop that sends the ResvConfirm messages uses the next RSVP-capable hop as the next IP hop for the packets and does not have the MAC address that is needed to encapsulate the IP packets for this next IP hop.

Workaround: Configure a static ARP entry that enables the router to properly encapsulate the packet by entering the **arp ip-address hardware-address arpa** command. The *ip-address* argument is the address of the next hop (that is visible via the RSVP debugs) for the ResvConfirm messages and the *hardware-address* argument is the MAC address of the interface of the next IP hop through which the ResvConfirm messages should be routed.

- CSCeg51291

Symptoms: A VRF ping fails to reach an OSPF neighbor interface.

Conditions: This symptom is observed when the platform on which the ping originates and the OSPF neighbor interface are connected via an OSPF sham link that is used for interconnecting traffic between two VPN sites.

Workaround: There is no workaround.

- CSCeg52659

Symptoms: A Cisco 7200 series may not withdraw a BGP route from an iBGP peer.

Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.3(3) when the **clear ip bgp neighbor-address soft out** command is entered for one of the members of the peer group of which the Cisco 7200 series is a member and when some changes to the outbound policy are made to the same member of the peer group. This situation causes some prefixes to remain struck in the other members of the peer group. The symptom may also occur in other releases.

The symptom is a very old behavior of the BGP peer group functionality: when one member of a peer group is cleared via either a hard reset or a soft reset and a policy change causes some of the prefixes to be withdrawn, inconsistencies may occur in the routes on the other members of the peer group.

Workaround: For peer groups and neighbors that are members of a peer group, do not enter the BGP neighbor-specific **clear ip bgp neighbor-address soft out** command or the **clear ip bgp neighbor-address** command. Rather, enter the peer group-specific **clear ip bgp peer-group-name soft out** command or the **clear ip bgp peer-group-name** command.

- CSCeg57155

Symptoms: A ping, Telnet traffic, FTP traffic, and trace route traffic across a VRF-aware NAT do not function.

Conditions: This symptom is observed on a Cisco router that is configured for VRF-aware NAT only when the router is not directly connected to a gateway.

Workaround: There is no workaround.

- CSCeh09588

Symptoms: During an NSF switchover on a RP, the convergence may be delayed up to five minutes.

Conditions: This symptom is observed when a DBD exchange error occurs while the adjacency is brought up.

Workaround: Enter the **clear ip ospf process** command on the affected router.

- CSCeh15639

Symptoms: A Cisco router may crash when it is reloaded with PIM traffic on the network.

Conditions: This symptom is observed on a Cisco 7200 series router with multicast enabled but is not platform dependent. Bootup is the most likely place where this will happen, but the router may crash anytime if an interface flap happens at the right time while receiving PIM traffic.

Workaround: There is no workaround.

- CSCeh33504

Symptoms: A router terminates 102,000 VPNv4 routes but route reflectors (RRs) report only a subset of the total.

Conditions: This symptom is observed on a Cisco MGX RPM-XF that runs Cisco IOS Release 12.3(11)T4 when 204 routes are configured per VRF over 496 VPNs (one VPN has about 1000 routes). However, Cisco MGX RPM-PRs that function as RRs show that only 76245 routes are terminated on the Cisco MGX RPM-XF. The symptom is platform-independent and may also occur in other releases.

Workaround: There is no workaround.

- CSCeh35246

Symptoms: A router may crash when a subinterface on which OSPF is running is deleted.

Conditions This symptom is observed when the **mpls ldp sync** command is configured under OSPF.

Workaround: There is no workaround.

- CSCeh35659

Symptoms: When the **ip bgp fast-external-fallover permit** interface configuration command is enabled on the main interface of a 4-port Gigabit Ethernet ISE line card and on a subinterface of a connected BGP neighbor, and when you enter the **shutdown** interface configuration command on the main interface, the BGP session that is established on the subinterface remains up for about 150 to 180 seconds before the BGP hold timer causes the session to go down.

Conditions: This symptom is observed on a Cisco 12000 series in a per-interface fast external fallover configuration on a 4-port Gigabit Ethernet ISE line card. However, the symptom may also occur on other platforms that function in a BGP configuration.

Workaround: There is no workaround. Note that the **ip bgp fast-external-fallover permit** command is currently not supported on subinterfaces.

- CSCeh53906

Symptoms: A stale non-bestpath multipath remains in the RIB after the path information changes, and BGP does not consider the stale path part of the multipath.

Conditions: This symptom is observed on a Cisco router that has the **soft-reconfiguration inbound** command enabled and occurs only when the BGP Multipath Loadsharing feature is enabled for three or more paths, that is, the *number-of-paths* argument of the **maximum-paths number-of-paths** command has a value of three or more.

Workaround: Disable the **soft-reconfiguration inbound** command for the neighbor sessions for which the BGP Multipath Loadsharing feature is enabled or reduce the maximum number of paths for the BGP Multipath Loadsharing feature to two.

- CSCeh66944

Symptoms: When you enable NSF for BGP, a BGP session flaps.

Conditions: This symptom is observed on a Cisco router that is configured for mVPN.

Workaround: Do not enable NSF if mVPN is also configured.

- CSCei06089

Symptoms: Conditional advertisement of the default route via a route map does not work when you enter the **neighbor default-originate** command.

Conditions: This symptom is observed on a Cisco router that is configured for BGP.

Workaround: Disable the route map entirely. If this is not an option, there is no workaround.

- CSCei13040

Symptoms: When an OSPF neighbor comes back up after a very fast (sub-second) interface flap, OSPF routes that are learned via the interface that flapped may not be re-installed in the RIB.

Conditions: This symptom is observed when the following two events occur:

- The interface flaps very quickly.
- The neighbor comes back up before the LSA generation timer expires.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface that flapped.

Alternate Workaround: Enter the **clear ip route * EXEC** command.

- CSCei16615

Symptoms: A neighbor reloads when you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on an interface of an LSP router that functions as a tunnel headend.

Conditions: This symptom is observed when the following events occur:

- The tunnel headend sends a Path via RSVP to the neighbor but the Resv message is delayed.
- There is only one Path to the neighbor for the session.
- At the neighbor, the cleanup timer for the Path expires before the Resv message arrives, causing the session to be terminated.

Workaround: There is no workaround.

- CSCei25442

Symptoms: The Border Gateway Protocol (BGP) multicast distribution tree (MDT) subaddress family identifier (SAFI) could send faulty notifications to Protocol Independent Multicast (PIM) resulting in a corrupted PIM database.

Conditions: This symptom has been observed when the BGP MDT SAFI receives BGP MDT SAFI rd 2 style updates.

Workaround: There is no workaround.

- CSCei25454

Symptoms: Connectivity loss may occur for MVPNs.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(30)S or a later release when the MVPNs function in a mixed network that has both VPNv4 RD2 prefixes for MDT updates and IPv4 MDT subaddress family identifier (SAFI) prefixes.

Workaround: There is no workaround.

- CSCei26899

Symptoms: When you reset a BGP peer, some prefixes are missing.

Conditions: This symptom is observed on a Cisco MGX8850 RPM-XF that runs Cisco IOS Release 12.3(11)T. However, the symptom is platform-independent and may also occur in other releases.

Workaround: There is no workaround.

- CSCei45669

Symptoms: An OSPF router may update and originate a new version of an LSA when it should flush the LSA.

Conditions: This symptom is observed on the originating router when it receives a self-originated MaxAge LSA before it can flush this LSA from its database. This symptom may occur under a rare condition when a neighboring router calculates that it has a newer copy of the LSA from the originating router and bounces the MaxAge LSA to the originating router.

Workaround: Enter the **clear ip ospf process** command.

- CSCei58597

Symptoms: When you enter the **show running-config** or **process-min-time** command, a spurious memory access or crash may occur.

Conditions: This symptom is observed on a Cisco router that is configured for OSPFv3.

Workaround: There is no workaround.

- CSCei65865

Symptoms: When an RSVP application (for example, the MPLS TE feature) sends an updated Path message to reflect a modification in its QoS request, the updated Path message may not be forwarded by a downstream RSVP-aware router.

Conditions: This symptom is observed when the downstream RSVP-aware router has two RSVP features configured: local policy and refresh reduction. The commands to configure these features are the **ip rsvp policy local** command and the **ip rsvp signalling refresh reduction** command, respectively.

When an RSVP reservation is established with a Path/Resv message handshake and the sender application subsequently transmits an updated Path message that the downstream router applies to an RSVP local policy, the router does not forward the modified Path message. This situation prevents the application from receiving the corresponding Resv message, and may cause the application to fail.

Workaround: If this is an option, unconfigure the local RSVP policy or refresh the reduction and then restart the RSVP application. If this is not an option, there is no workaround.

- CSCei75375

Symptoms: OSPFv3 may write zeros into single words of memory in the heap. Depending on what (if anything) is allocated at the address that is being cleared, the router may reload or fail in some other way.

Conditions: This symptom is observed only when an OSPFv3 process or area is unconfigured or when you enter the **clear ipv6 ospf process** command and when both of the following conditions are present:

- The area that is removed or the process that is cleared contains one or more non-self-originated type-4 LSAs.
- The router does not have an intra-area path to an ASBR that is described by the type-4 LSA.

Workaround: There is no workaround.

- CSCei77227

Symptoms: A Cisco router that functions in a multicast VPN environment may crash.

Conditions: This symptom is observed when you check the unicast connectivity and then unconfigure a VRF instance.

Workaround: There is no workaround.

- CSCei83265

Symptoms: MVPN traffic is limited to about 9 Mpps and the CPU usage on the egress line card is 100 percent.

Conditions: This symptom is observed on a Cisco router that functions as a PE router when MVPN performs decapsulation in the slow path instead of the fast path.

Workaround: There is no workaround.

- CSCei86031

Symptoms: When the **distribute-list route-map map-tag** command is used under the OSPF router mode and when the route map is modified, OSPF does not update the routing table based on the changes in the route map.

Conditions: This symptom is observed when a route map that is referenced in the **distribute-list route-map map-tag** command is modified.

Workaround: Enter the **clear ip ospf process id** command or the **clear ip route *** command.

- CSCsa57101

Symptoms: A Cisco router may reload when the RSVP MIB object is polled via SNMP.

Conditions: The symptom is platform- and release-independent.

Workaround: Disable SNMP by entering the **no snmp-server host** command.

- CSCsa75512

Symptoms: A crash that is related to OSPF flooding may occur on a Cisco router that is configured for OSPF and MPLS traffic engineering.

Conditions: This symptom is observed when 1600 OSPF interfaces are configured in an OSPF area that is also configured for MPLS traffic engineering and when OSPF interfaces and OSPF adjacencies flap. A list of the affected releases can be found at <http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CScef16096>. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

Workaround: Reduce the number of OSPF interfaces in the OSPF area to 300 or less. You can check the number of OSPF interfaces by entering the **show ip ospf** or **show ip ospf interface interface-type interface-number brief** command. Note that all interfaces that are covered by network statements are counted.

- CSCsa87473

Symptoms: A BGP speaker may fail to send all of its prefixes to a neighbor if the neighbor sends a refresh request to the BGP speaker at the same time that the BGP speaker is generating updates to the neighbor. This situation causes the neighbor to miss some prefixes from its BGP table.

Conditions: This symptom may occur between any pair of BGP speakers.

A common scenario is that a VPNv4 PE router is reloaded and then fails to learn all prefixes from its route reflector (RR). In this configuration, the symptom occurs when the processing of a VRF configuration causes the PE router to automatically generate a route-refresh request to the RR, while the RR is still generating updates to the PE.

Workaround: There is no workaround.

- CSCsa95973

Symptoms: After a switchover, secondary traffic loss occurs for OSPF routes.

Conditions: This symptom is observed when OSPF NSF is configured on an ABR and when a prefix can be learned via an “Area 0” link or via a link through another area (that is, there are redundant paths).

Workaround: There is no workaround.

- CSCsa98059

Symptoms: Suboptimal routing occurs in an OSPF configuration or a routing loop occurs between two border routers that redistribute BGP into OSPF.

Conditions: These symptoms are observed when at least two border routers are connected via eBGP to another autonomous system, receive the same prefix over these connections, and redistribute the prefix into OSPF. Under certain conditions, for example when the eBGP session from the preferred BGP exit point to the eBGP peer flaps, the second router in the local autonomous system becomes the preferred path and redistributes the eBGP route into OSPF. When the eBGP session with the first router comes back up, the LSA should be flushed but this does not occur. This situation may create routing problems on other OSPF routers or, when BGP has a higher administrative distance than OSPF, routing loops between both border routers.

Workaround: There is no workaround.

- CSCsb01490

Symptoms: When general Bidirectional Forwarding Detection (BFD) functionality is enabled and when Border Gateway Protocol (BGP) is configured without BFD functionality, BFD sessions may be started with the BGP neighbors. This is not proper behavior: BFD sessions should not be started when BGP is configured without BFD functionality.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(31)S.

Workaround: There is no workaround.

- CSCsb09852

Symptoms: The number of networks in the BGP table and the number of attributes increases, and a slower convergence may occur for members of a BGP update group.

Conditions: This symptom is observed on a Cisco router when the members of a BGP update group go out of synchronization with each other in such a way that they have different table versions, preventing the BGP Scanner from freeing networks that do not have a path.

To check if the members of the BGP update group are in synchronization with each other, enter the **show ip bgp update-group summary** command and look at the table version for each member. If they have the same table version, they are in synchronization with each other; if they do not, they are out of synchronization with each other.

Workaround: To enable the members of the BGP update group to synchronize with each other, enter the **clear ip bgp * soft out** command. Doing so does not bounce the sessions but forces BGP to re-advertise all prefixes to each member.

- CSCsb36589

Symptoms: A router that is configured for OSPFv3 may crash because of memory corruption or a CPUHOG condition.

Conditions: This symptom is observed rarely in a configuration with a large LSA with at least 44 links that have OSPFv3 enabled and with some links configured for broadcast mode when an adjacency with a peer router flaps.

Workaround: There is no workaround.

- CSCsb36755

Symptoms: When BGP receives an update that has a worse metric route than the previously received route for equal-cost multipath, the BGP table is updated correctly but the routing table is not, preventing the old path from being deleted from the routing table.

Conditions: This symptom is observed on a Cisco router that is configured for BGP multipath.

Workaround: Enter the **clear ip route network** command.

- CSCsb51101

Symptoms: When you perform an SSO switchover, packets may be lost because of a “no route” condition. The loss of these packets is an indication of a prolonged SSO convergence time. The routes for these packets are restored automatically within a few seconds.

Conditions: This symptom is observed on a Cisco router with dual RPs that function in SSO mode.

Workaround: There is no workaround.

- CSCsb54823

Symptoms: One router (R2) may begin sending updates to another router (R1) before R2 has received the BGP prefix list from R1.

R1 does apply its inbound BGP prefix list so routes are denied if they need to be. However, R2 sends routes to R1 which are denied by R1.

Conditions: This symptom is observed when both routers have negotiated a BGP outbound route filter (ORF) and when R1 sends its BGP prefix list to R2.

Workaround: There is no workaround.

- CSCsb60206

Symptoms: When an SSO switchover occurs, the newly active Supervisor Engine or RP generates a series of CPU Hog messages in the PIM Process, generates tracebacks, and finally crashes because the watchdog timer expires.

Conditions: This symptom is observed on a Cisco switch that has redundant Supervisor Engines and on a Cisco router that has redundant RPs when Auto-RP is configured and when regular multicast traffic runs for a few hundred multicast routes.

Workaround: There is no workaround.

- CSCsb64585

Symptoms: A Rendezvous Point is down but multicast routing continues to function.

Conditions: This symptom is observed when a statically mapped Rendezvous Point is defined as an interface address and when the interface is in the down/down state. In this situation, the router still attempts to become the Rendezvous Point for the defined group or groups.

Workaround: Do not use a statically mapped Rendezvous Point. Rather, configure Auto-RP or BSR to configure a dynamic Rendezvous Point.

- CSCsb74588

Symptoms: A router that is configured for OSPFv3 may crash because of memory corruption or a CPUHOG condition.

Conditions: This symptom is observed rarely in a configuration with a large LSA with 64 parallel links that have OSPFv3 enabled in broadcast mode when all adjacencies with a peer router flap.

Workaround: There is no workaround.

- CSCsb74708

Symptoms: An OSPF sham link may not form an adjacency.

Conditions: This symptom is observed when there is an interface in the global route table that has an IP address that matches the IP address of the OSPF sham link neighbor.

Workaround: Reconfigure the routers so that the IP address of the OSPF sham link neighbor does not match any IP addresses of interfaces in the global route table.

Alternate Workaround: Shut down the interface or change the IP address of the interface in the global route table.

- CSCsb79749

Symptoms: The output of the **show memory summary** command may contain garbled characters in the "What" column.

Conditions: This symptom is observed when you configure OSPF with at least one network, and then unconfigure it.

Workaround: There is no workaround.

- CSCsc07467

Symptoms: An OSPF route is lost after an interface flaps.

Conditions: This symptom is observed rarely when all of the following conditions are present:

- There is a very brief (shorter than 500 ms) interface flap on a point-to-point interface such as a POS interface.
- The flap is not noticed by the neighbor, so the neighbors interface remains up.
- The OSPF adjacency goes down and comes back up very quickly (the total time is shorter than 500 ms).
- OSPF runs an SPF during this period and, based on the transient adjacency information, removes routes via this adjacency.
- The OSPF LSA generation is delayed because of LSA throttling. When the LSA throttle timer expires and the LSA is built, the LSA appears unchanged.

Workaround: Increase the carrier-delay time for the interface to about 1 second or longer.

Alternate Workaround: Use an LSA build time shorter than the time that it takes for an adjacency to come up completely.

- CSCsc10494

Symptoms: When an inter-area, external, or Not-So-Stubby Area (NSSA) route is learned via a link state update that follows the initial database synchronization, the route may not be added to the routing table by a partial shortest path first (SPF) computation even though the LSA is installed in the link state database. A subsequent full SPF computation causes the route to be added.

Conditions: This symptom is observed on a Cisco router and is most likely to occur when a large number of type 3, type 5, or type 7 LSAs are advertised and withdrawn.

Workaround: Trigger an action that causes a full SPF computation.

- CSCsc36517

Symptoms: A router reloads unexpectedly when a continue statement is used in an outbound route map.

Conditions: This symptom is observed on a Cisco router that is configured for BGP.

Workaround: There is no workaround.

- CSCsc49741

Symptoms: A router may crash when OSPFv3 is enabled.

Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS software image that integrates the fix for caveat CSCei47926. A list of the affected releases can be found at <http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCei47926>. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

Workaround: There is no workaround.

- CSCsc59089

Symptoms: BGP does not advertise all routes to a peer that sends a route-refresh request.

Conditions: This symptom is observed under the following conditions:

- The router is in the process of converging all of its peers and has updates ready in the output queue for the peer.
- The peer sends a route-refresh request to the router. This may occur when the **clear ip bgp * soft in** command is entered on the peer or when a VRF is added to the peer.
- The router processes the route-refresh request from the peer while the router still has updates in the output queue for the peer.

In this situation, all of prefixes that are advertised by the unsent updates in the output queue for the peer are lost.

Workaround: There is no workaround. When the symptom has occurred, enter the **clear ip bgp * soft out** command on the router to force the router to send all updates to its peers.

ISO CLNS

- CSCeh00090

Symptoms: Routes may be unexpectedly removed from the routing table.

Conditions: This symptom is observed when IS-IS is used to advertise IP prefixes and when you enter a **distance** command that changes the overall configuration but keeps a subset of the prefixes at the same distance as in the previous configuration. The routes for which the distance does not change may be removed from the routing table.

The following two examples show configurations in which the symptom occurs. When the distance configuration for IS-IS is **115 ip** and you enter one of the following command sequences, the symptom occurs:

```
router isis
  distance 255 ip
  distance 115 ip
or
router isis
  distance 115 0.0.0.0 255.255.255.255
```

Workaround: For all prefixes, configure distances that differ from the distances that were initially configured.

- CSCeh41328

Symptoms: IPv6 routes that are learned from other IPv6 routers are not installed in the RIB.

Conditions: This symptom is observed on a Cisco router that is configured for Multi-topology IS-IS in transition mode. This symptom does not occur when the router is configured for Multi-topology IS-IS without the transition mode.

Workaround: Use the default IS-IS metric on the interfaces that are configured for IPv6 IS-IS.

- CSCeh61778

Symptoms: A Cisco device running IOS and enabled for Intermediate System-to-Intermediate System (IS-IS) routing protocol may reset with a SYS-2-WATCHDOG error from a specifically crafted malformed IS-IS packet. The IS-IS protocol is not enabled by default.

Conditions: The IS-IS crafted malformed IS-IS Packet that requires processing will not be forwarded across a Level 1/Level 2 boundary. The specifically crafted malformed IS-IS packet would require local attachment to either a Level 1 or Level 2 router. A Cisco device receiving the malformed IS-IS packet will forward the malformed packet to its neighbors, and may reset.

Workaround: There is no workaround. Enabling IS-IS Authentication is seen as a best practice, and can be leveraged as a mitigation technique.

- CSCei04683

Symptoms: A router may advertise an IPv6 default route into a level-2 topology.

Conditions: This symptom is observed when the following conditions are present:

- The router runs the IS-IS routing protocol on both level 1 and level 2.

- The router advertises IPv6 prefixes.
- The router has the IS-IS ATT bit set.
- The router has level-1 connectivity to another level-1/level-2 IS-IS router.
- An SSO switchover occurs on the router or the router loses and then regains connectivity to the level-2 topology.

Workaround: Trigger a change that causes the router to regenerate its level-2 LSP.

- CSCei12603

Symptoms: A 30 to 40 ms interruption in traffic forwarding may occur when you modify the **tunnel mpls traffic-eng bandwidth** command for an MPLS traffic-engineering tunnel.

Conditions: This symptom is observed on a router that is configured for MPLS traffic engineering with IS-IS as the associated IGP.

Workaround: There is no workaround.

- CSCei58655

Symptoms: A route that fails remains in the routing table with its old metric, preventing an alternate route from being used and causing a routing loop.

Conditions: This symptom is observed in a network that is configured for IS-IS and iSPF when the IP routes that are advertised in an LSP (irrespective of whether or not the LSP is fragmented) do not age-out during a rerouting failure.

Workaround: Remove iSPF from the IS-IS process by entering the **router isis** command followed by the **no ispf** command.

- CSCsb07279

Symptoms: When an IPv4 prefix list is used in a redistribution command for the IS-IS router process, a change in the prefix list is not immediately reflected in the routing tables of a router and its neighbor. The change may take up to 15 minutes to take effect.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(28)S.

Workaround: To have a change take effect immediately, enter the **no redistribute route-map** command followed by the **redistribute route-map** command for the IS-IS router process.

- CSCsb34032

Symptoms: A router may reload unexpectedly when you remove the IS-IS configuration at the interface or router level.

Conditions: This symptom is observed on a Cisco router when the following conditions are present:

- The router is HA-capable.
- The **isis protocol shutdown** interface configuration command is enabled on the interface.
- You enter an interface configuration command that enables IS-IS such as an **isis** command, a **clsns** command, or the **ipv6 router isis** before you enter the a router configuration command such as the **net** command.

When you now remove the IS-IS configuration at the interface or router level, the router may reload.

Workaround: Remove the **isis protocol shutdown** interface configuration command before you remove IS-IS from the interface or router level.

Miscellaneous

- CSCdr52721

Symptoms: Temporary performance degradation may occur on a router, and the following error message is generated:

```
%SYS-3-CPUHOG: Task ran for 2064 msec (348/253), process = Per-minute Jobs.
```

Conditions: This symptom is observed on a Cisco 7200 series that is configured with a large number of PVCs.

Workaround: There is no workaround.

- CSCdr54486

Symptoms: Traffic is dropped for up to 15 seconds while a recursive prefix is being resolved.

Conditions: This symptom is observed when a new recursive prefix is learned by CEF and when a less-specific prefix already exists. Traffic that would have been forwarded using the less-specific prefix is dropped for up to 15 seconds while the new recursive prefix is being resolved.

Workaround: There is no workaround.

- CSCdz83100

Symptoms: High CPU use may occur at the interrupt level on an ingress port adapter or line card that is configured for hardware multicast when there is a high multicast traffic rate.

Conditions: This symptom is observed when policy-based routing (PBR) matches the multicast traffic and when a switchover to another interface occurs.

Workaround: Change the deny statement in the PBR configuration so traffic for multicast destination addresses is denied earlier.

Alternate Workaround: For a short while, remove the PBR configuration from the ingress interface to enable multicast traffic hardware forwarding to be established.

Further Problem Description: PBR should not influence multicast traffic and it does not when traffic is switched in the hardware. When a switchover to a new interface occurs, multicast packets are initially forwarded in the software until hardware forwarding can take over. PBR interferes with the initial software-switched packets and prevents hardware entries from being created.

- CSCea11344

Symptoms: The **atm abr rate-factor** interface configuration command cannot be configured on an interface.

Conditions: This symptom is observed when an available bit rate (ABR) connection is added to a Route Processor Module-PRemium (RPM-PR) card on a Cisco MGX 8850 Processor Switch Module (PXM1) card that has a Cisco WAN Manager (CWM) carrier module (CM). The symptom may also occur on other platforms.

Workaround: Use the command-line interface (CLI) to add an ABR connection to the RPM-PR on the Cisco MGX 8850 PXM1 card.

- CSCeb66825

Symptoms: A Cisco 7200 series may reload unexpectedly during a service-policy configuration.

Conditions: This symptom is observed when you attach a level 2 policy map as a child of a level 1 policy map and when the level 1 policy map is already attached to an interface.

Workaround: Create a level 3 policy map, and attach it to the interface.

- CSCec65977

Symptoms: A 4-port serial enhanced port adapter (PA-4T+) may receive packets, even though the status of the serial interface is “down/down.”

Conditions: This symptom is observed on a PA-4T+ that is installed in a Cisco 7200 series router and that is connected to a 1-port serial WAN interface card (WIC-1T) that is installed in a Cisco 2600 series. The serial interfaces of both routers are connected with a CSU/DSU.

The input packet counter of the serial port of the PA-4T+ increments even though the status of the serial interface is “down/down.” However, the 2600 series functions properly, and the input packet counter of its serial interface does not increment.

Possible Workaround: Administratively shut down the serial port.

- CSCee48782

Symptoms: An Engine 4 or Engine 4+ line card in a Cisco 12000 series that switches multicast traffic may reload.

Conditions: This symptom is observed on a Cisco 12000 series when the **ip multicast-routing distributed** command is configured.

Workaround: Configure an access control list (ACL) to block ingress traffic with a source address of 0.0.0.0, as in the following example:

```
access-list 1 deny 0.0.0.0
access-list 1 permit any
interface pos3/0
    ip access-group 1 in
```

Note that this ACL does not have any effect on multicast traffic because multicast traffic with source address 0.0.0.0 is dropped anyway by the Reverse Path Forwarding (RPF) check.

- CSCee93598

Symptoms: An LSP ping reports that an LSP is fine although the LSP is unable to carry MPLS payloads such as VPN traffic.

Conditions: This symptom is observed on a Cisco router when MPLS echo request packets are forwarded from untagged interfaces that are directly connected to the destination of the LSP ping and when the IP time-to-live (TTL) value for the MPLS echo request packets is set to 1.

Workaround: There is no workaround.

- CSCef02056

Symptoms: An inter-AS TE tunnel continues to resignal a path that is rejected instead of switching to a second path.

Conditions: This symptom is observed when the RSVP local policy on the ASBR rejects the path message because it does not meet the policy.

Workaround: There is no workaround.

- CSCef08173

Symptoms: A VIP in which a PA-2FE port adapter is installed may reload because of memory corruption that is caused by a hardware issue of the PA-2FE port adapter.

Conditions: This symptom is observed when the VIP and port adapter function under stress, when the VIP is unable to serve memory read/write requests from the port adapter, and when there are PCI retry timeouts.

Workaround: There is no workaround.

- CSCef35269

Symptoms: A Cisco 7500 series that has a multichannel E1 port adapter that is configured with PPP multilink groups on several E1 channels may drop packets:

- When dCEF is enabled, packets that are larger than 1492 bytes are dropped. Note that this particular symptom is addressed and fixed via CSCin73658.
- When the router has dCEF disabled, packets that are larger than 1500 bytes are dropped.

Conditions The symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(28)S.

Workaround: Configure only one interface as the member of the PPP multilink group. Note that the symptom does not occur in Release 12.0(26)S3, 12.0(27)S2, and 12.1(19)E1.

- CSCef39223

Symptoms: A secondary RSP may fail to become active.

Conditions: This symptom is observed on a Cisco 7500 series that functions in an SSO configuration when you perform an OIR of the primary RSP.

Workaround: Do not perform an OIR of the primary RSP.

- CSCef75174

Symptoms: A router may crash when you enter the **dir flash:** command.

Conditions: This symptom is observed on a low-end router that uses a Compact Flash (CF) device when the root directory is nearly full with file entries.

Workaround: Keep the number of file entries in the root directory relatively small (less than 100).

- CSCef79749

Symptoms: APS does not function correctly on a channelized OC-48 ISE line card and the output of the **show aps** command shows that the line card is down.

Conditions: This symptom is observed on a Cisco 12000 series.

Workaround: There is no workaround.

- CSCef87449

Symptoms: When you enter the **shutdown** interface configuration command on the outgoing interface of a Traffic Engineering (TE) Label Switched Path (LSP), the Resv state should be removed immediately. However, the Resv state remains until a PathTear arrives or a timeout causes the TE LSP to be torn down.

When the TE headend is a Cisco router, the PathTear is sent very quickly and the state is removed.

This symptom is short-lived and it is very unlikely to be noticed.

Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS software image that contains the fix for caveat CSCec26563 when the router has MPLS TE tunnels enabled.

A list of the affected releases can be found at

<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCec26563>. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

Workaround: There is no workaround.

- CSCef95861

Symptoms: IPv6 packets may be incorrectly forwarded by a Cisco 10720 or packet forwarding performance may be degraded significantly. Traceroute packets may be misrouted or high CPU use may occur when IPv6 packets are punted to the Route Processor.

Conditions: These symptoms are observed on a Cisco 10720 that runs Cisco IOS Release 12.0(27)S1.

Workaround: There is no workaround.

- CSCeg07617

Symptoms: The following error message and spurious memory access may be generated on a Cisco 7500 series or Cisco 7600 series that is configured for dMLFR.

```
%ALIGN-3-SPURIOUS: Spurious memory access made at 0x418FC0E0 reading 0x8
%ALIGN-3-TRACE: -Traceback= 418FC0E0 4026B644 40699284 40699A3C 40699368 40E80B84
40E7215C 4068A8AC
```

Conditions: This symptom is observed immediately after an MFR interface is created, after a switchover has occurred, or when a link flaps continuously.

Workaround: There is no workaround.

- CSCeg12134

Symptoms: When you send multicast traffic over an IPsec tunnel, a memory leak may occur on a router.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3T when both IP CEF and hardware encryption are configured. The symptom may also occur in other releases.

Workaround: Switch to software encryption for a while and then switch back to hardware encryption.

Alternate Workaround: Disable IP CEF.

- CSCeg21548

Symptoms: A router crashes when you enter the **show bfd neighbors** command.

Conditions: This symptom is observed on a Cisco platform while BFD sessions flap.

Workaround: There is no workaround.

- CSCeg24422

Symptoms: Packet drops occur in the ingress direction on a dMLP or dMLFR link with traffic at 95-percent of the line rate and when the number of packets with a small size is high.

Conditions: This symptom is observed on a Cisco 7500 series that functions as a provider edge (PE) router, that is configured for L2TPv3 L3VPN, and that has dMLP or dMLFR links to a customer edge (CE) router.

Workaround: There is no workaround.

- CSCeg26528

Symptoms: The performance of a router may be severely degraded (at approximately 90 percent of the line rate) when large packets are processed, when the MLP bundle link flaps, and when the router does not recover the MLP sequence numbers of the packets.

Conditions: This symptom is observed on a Cisco 7500 series and Cisco 7600 series that are configured for dMLP only when large packets are processed.

Workaround: There is no workaround.

- CSCeg35670

Symptoms: Shortly after a Cisco IOS software boot loader image has been downloaded, a PRP-2 may crash and does not reload.

Conditions: This symptom is observed on a Cisco 12000 series that runs the boot loader image of Cisco IOS Release 12.0(30)S.

Workaround: There is no workaround.

- CSCeg46980

An 8-port OC-48c/STM-16c POS Engine 6 line card may report the error following messages, indicating that the Rx power has exceeded the alarm levels for the port:

```
SLOT X: %LC_SFP-2-SFP_RX_POWER_HI_ALARM: RX power high alarm
SLOT X: %LC_SFP-4-SFP_EVENT_TX_FAULT: TX FAULT signal raised on port Y
SLOT X: %LC_SFP-4-SFP_EVENT_TX_FAULT: TX FAULT signal cleared on port Y
```

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(27)S2 or Release 12.0(31)S.

Workaround: There is no workaround.

- CSCeg49872

Symptoms: After a line card crashes, the crashinfo file may be saved to bootflash with a size of 0 bytes.

Conditions: This symptom is observed on a Cisco 12000 series.

Workaround: There is no workaround. To troubleshoot the crash, enter the **show bootflash: all** to see the logs of the event.

- CSCeg57219

Symptoms: You cannot ping with packets of certain sizes after an RPR+ switchover or after an interface flap on a multilink interface that has members of non-channelized port adapters when the multilink interface is configured with fragmentation and interleaving.

Conditions: This symptom is observed on a Cisco 7500 series and Cisco 7600 series.

Workaround: There is no workaround.

- CSCeg64331

Symptoms: When you change the MTU on a serial interface, the standby Route Processor (RP) generates tracebacks, enters the STANDBY COLD-CONFIG state, and reboots.

Conditions: This symptom is observed on a Cisco router when you change the MTU size to 1400 or a lesser value.

Workaround: There is no workaround.

- CSCeg70593

Symptoms: The ATM interface route cache counters do not increment after you have entered the **ip cef** command.

Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS interim release for Release 12.0(31)S, that functions as a PE router, and that has L2 transport VCs configured.

Workaround: There is no workaround.

- CSCeg74562

Symptoms: A router may take a very long time to establish LDP sessions with its peers and advertise its label bindings. In some cases, the LDP sessions may flap.

Conditions: This symptom may occur when a Cisco router that uses LDP for label distribution has a large number (greater than 250) of LDP neighbors and several thousand label bindings to advertise.

Workaround: The time required to establish the neighbor sessions and advertise the label bindings when TDP is used in place of LDP may be substantially less. Using TDP in place of LDP will result in an acceptable convergence behavior.

- CSCeg76795

Symptoms: L2TPv3 sessions are re-established after their L2TP class has been deleted.

Conditions: This symptom is observed when you enter the **no l2tp-class** global configuration command to delete the class that is used by existing Xconnect paths via a pseudowire class.

Workaround: Remove the Xconnects paths along with the L2TP class.

- CSCeg83164

Symptoms: A router may reload when you configure an ATM VC class.

Conditions: This symptom is observed on a Cisco 7200 series and Cisco 7500 series that are configured for MPLS but may be platform-independent.

Workaround: There is no workaround.

- CSCeg83460

Symptoms: Bidirectional PIM DF election does not occur correctly when a PIM neighbor expires.

Conditions: This symptom is observed when the PIM neighbor that expires is the designated forwarder (DF) for multiple RPs. The DF election is triggered only for the first RP on the list and does not occur for all the other RPs.

Workaround: Clear the state of the DF or toggle the interface state of the DF.

- CSCeh05988

Symptoms: A CSC OIR may cause a 6-port channelized T3 line card that is configured for FRoMPLS to fail.

Conditions: This symptom is observed on a Cisco 12000 series that runs a Cisco IOS interim release for Release 12.0(31)S and that has its redundancy mode set to RPR.

Workaround: There is no workaround.

- CSCeh12675

Symptoms: Traffic may not fully converge after you have reloaded a line card with a scaled configuration or after an HA switchover.

Conditions: This symptom is observed on a Cisco 12416 that runs the c12kprp-p-mz image of a Cisco IOS interim release for Release 12.0(31)S and that is configured with dual PRPs and a scaled configuration.

Workaround: There is no workaround.

- CSCeh13340

Symptoms: On a Cisco XR 12000 series hardware-based forwarding line card, the receive counters in the output of the **show mpls l2transport vc** command do not work in any images for AToM.

Conditions: This symptom is observed on all hardware-based engine line cards on a Cisco XR 12000 series that is configured for AToM and Sampled NetFlow on the core-facing line cards.

Workaround: There is no workaround.

- CSCeh14012

Symptoms: A 1-port channelized OC-12/STM-4 (DS1/E1) ISE line card on a CE router may crash when many (168) MLP interfaces are deleted and reconfigured via TFTP on a directly-connected PE router.

Conditions: This symptom is observed on a Cisco 1200 series that functions as a CE router.

Workaround: There is no workaround.

- CSCeh18195

Symptoms: Packets that flow to VPNv4 destinations may be dropped for up to one second when the next-hop router clears its IS-IS overload bit after having been rebooted.

Conditions: This symptom is observed in a MPLS-TE network with one-hop TE tunnels.

Workaround: There is no workaround.

- CSCeh20156

Symptoms: When the working link flaps with two to three second intervals on CHOC12 Internet Services Engine (ISE) line cards that are configured for automatic protection switching (APS), some T1 links may remain down.

Conditions: This symptom is observed on a Cisco 12000 series.

Workaround: Reload the line card(s).

- CSCeh25739

Symptoms: High jitter occurs on a 1-port channelized OC-12/STM-4 (DS1/E1) ISE line card when many (168) MLP interfaces are congested with real-time and normal data traffic.

Conditions: This symptom is observed on a Cisco 12000 series.

Workaround: There is no workaround.

- CSCeh29183

Symptoms: When you configure MPLS Traffic Engineering AutoTunnel Mesh Groups by entering the following commands, many FIB messages and tracebacks are generated:

```
mpls traffic-eng auto-tunnel mesh
mpls traffic-eng auto-tunnel mesh tunnel-num min 10000 max 20000
```

Depending on the configuration of the router and the topology, the symptom may also occur when you enter the following sequence of commands:

```
no mpls traffic-eng auto-tunnel mesh
mpls traffic-eng auto-tunnel mesh
no mpls traffic-eng auto-tunnel mesh
mpls traffic-eng auto-tunnel mesh
```

Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of a Cisco IOS interim release for Release 12.0(31)S.

Workaround: When you want to disable and then re-enable the **mpls traffic-eng auto-tunnel mesh** command, save the configuration and reload the router after you have disabled the command and before you re-enable the command, as in the following example:

```
no mpls traffic-eng auto-tunnel mesh
...
copy run start
reload
mpls traffic-eng auto-tunnel mesh
```

Similarly, when you want to change the range of unit numbers (that is, tunnel IDs) that is used by the **mpls traffic-eng auto-tunnel mesh** command, disable the command, change the range, save the configuration, reload the router, and then re-enable the command, as in the following example:

```
no mpls traffic-eng auto-tunnel mesh
mpls traffic-eng auto-tunnel mesh tunnel-num min 10000 max 20000
...
copy run start
reload
mpls traffic-eng auto-tunnel mesh
```

- CSCeh31691

Symptoms: Changing the encapsulation of a POS interface from HDLC to PPP or the other way around causes the link to go down.

Conditions: This symptom is observed when you change the encapsulation of a POS interfaces on an Optical Services Module (OSM) that is installed in a Cisco Catalyst 6000 series or Cisco 7600 series. However, the symptom is platform-independent.

Workaround: Power-cycle the OSM by entering the **no power enable module slot** command followed by the **power enable module slot** command.

- CSCeh32706

Symptoms: An inter-AS TE LSP fails to send a signal after a router is rebooted as an ASBR.

Conditions: This symptom is observed when there are parallel links between ASBRs with a combination of point-to-point and broadcast interfaces that are configured with the MPLS Traffic Engineering—Inter-AS TE feature and (passive) link flooding.

Workaround: Shut down the broadcast interface between the ASBRs.

- CSCeh35411

Symptoms: A line card or port adapter may crash repeatedly when the router in which the line card or port adapter is installed comes up after a software-forced crash has occurred on the router.

Conditions: This symptom is observed on a Cisco router that is configured for IPv6 MPLS and that has redundant RPs that are configured for SSO. The symptom is more likely to occur when the **ipv6 unicast-routing** command is enabled.

Workaround: To diminish the chance that the symptom occurs, disable the **ipv6 unicast-routing** command.

- CSCeh35422

Symptoms: A PRP switchover causes “%SYS-2-NOTQ” and “%SYS-2-LINKED” error messages and some tracebacks to be generated on a 1-port channelized OC-12c/STM-4 (DS1/E1) ISE line card, the serial interfaces of the line card flap, and eventually the line card resets.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S or Release 12.0(30)S, that is configured with two PRPs, and that has the redundancy mode set to SSO.

Workaround: There is no workaround.

- CSCeh37351

Symptoms: In the a tag switching-to-IP switching scenario with an ISE ingress line card and an Engine 4 plus (E4+) egress line card, the following bad packets may be forwarded to the E4+ line card:

- tag2ip, with bad ip hdr cksum
- tag2ip, with ip->tl > L2

- tag2ip, with ip->tl < 20
- tag2ip, with ip options packets
- tag2ip, with ip options packets with bad ip hdr cksum
- tag2ip, with ip options packets with ip->tl > L2
- tag2ip, with ip options packets with ip->tl < 20

These bad packets cause packet corruption and a “TX192-3-PAM_PIM” error message on the E4+ line card and may even cause the E4+ line card to reset.

Conditions: This symptom is observed on a Cisco 12000 series.

Workaround: There is no workaround.

Further Problem Description: The fix for this caveat enables the ISE line card to drop the above-mentioned bad packets.

- CSCeh39850

Symptoms: When an attachment circuit is configured for AToM pseudowire redundancy, an MPLS core network failure on the primary pseudowire may not cause a switchover to the redundant (or backup) pseudowire.

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.2(27)SBA and on a Cisco 12000 series that runs a Cisco IOS interim release for Release 12.0(31)S.

Workaround: There is no workaround.

- CSCeh39904

Symptoms: After removing a large number of Frame Relay subinterfaces, the following log is displayed:

```
SYS-3-CPUHOG: Task ran for 38160 msec (3/2), process = MDFC LC Process, PC = 41129150
```

Conditions: This symptom is observed on a Cisco 12000 series that is configured for Multicast VPN.

Workaround: There is no workaround.

- CSCeh40556

Symptoms: Links flap on a 1-port channelized OC-12/STM-4 (DS1/E1) ISE line card after an RP switchover has occurred.

Conditions: This symptom is observed on a Cisco 12000 series that has two PRPs and that runs Cisco IOS Release 12.0(31)S.

Workaround: There is no workaround.

- CSCeh40882

Symptoms: On a Cisco 12000 series router with a 1xChOC12/DS1 ISE line card configured with multilink MFR protocol and a MQC policy, after a reload the QoS does not get applied to the bundle. The QoS goes to the suspend mode.

Conditions: The bundle loses its QoS policy when the router is reloaded. This problem is observed when running Cisco IOS Releases 12.0(28)S1, 12.0(30)S, or an interim release for Release 12.0(31)S.

Workaround: Remove the service-policy from the bundle and re-apply it.

- CSCeh41272

Symptoms: After you perform an OIR of a PA-SRP-OC12 port adapter on a Cisco 7200 series, the router may not show any nodes in the SRP ring and may stop forwarding traffic.

Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.3(13) or Release 12.3(11)T3. The symptom may also occur in other releases.

Workaround: There is no workaround.

- CSCeh42248

Symptoms: Some %GSRSPA-3-PORT_IF_INDEX & %EELC_QOS_RES_MGR-3-HW_IDB_INDEX_NOT_FOUND messages may be seen on Engine 5 Gigabit Ethernet (GE) Shared Port Adapters (SPAs) when an MPLS traffic engineering tunnel is enabled on the interface.

Conditions: This symptom is observed on an Engine 5 GE SPA in a Cisco 12000 series router that is running Cisco IOS Release 12.0(31)S.

Workaround: There is no workaround.

- CSCeh42465

Symptoms: An Engine 3 line card sends unlabeled traffic after it has been toggled from explicit routing to default routing. The symptom is related to the handling of a default-route on an Engine 3 ingress line card that functions in an IP-to-MPLS path.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(30)S1 or any other image that includes the fix for caveat CSCsa64782, which is a preliminary requisite for default-route handling on an Engine 3 line card. The symptom occurs in the following scenario:

1. You configure BGP to advertise the target address, so the target address is directly known in the routing table.
2. You remove the advertisement from BGP and return to default routing, with the same source for the next hop as the platform that was the BGP next hop.
3. You enter the **clear ip route network** command, with the address of the BGP next hop for the *network* argument.

After the transition from non-default routing to default routing, entering the **clear ip route network** command, with the address of the next hop for the *network* argument, causes an inconsistency, and traffic is forwarded as unlabeled.

Workaround: To restore proper operation, enter the **clear ip route 0.0.0.0** command.

- CSCeh49881

Symptoms: In a tag switching-to-IP switching scenario with an ISE ingress line card and an Engine 4 plus (E4+) egress line card, the following bad packets may be forwarded to the E4+ line card:

- tag2ip, with bad ip hdr cksum
- tag2ip, with ip->tl > L2
- tag2ip, with ip->tl < 20
- tag2ip, with ip options packets
- tag2ip, with ip options packets with bad ip hdr cksum
- tag2ip, with ip options packets with ip->tl > L2
- tag2ip, with ip options packets with ip->tl < 20

These bad packets cause packet corruption and a “TX192-3-PAM_PIM” error message on the E4+ line card and may even cause the E4+ line card to reset.

Conditions: This symptom is observed on a Cisco 12000 series.

Workaround: There is no workaround.

Further Problem Description: The fix for this caveat enables the ISE line card to drop the above-mentioned bad packets.

- CSCeh49892

Symptoms: The following incorrect error message is generated when an invalid QOS policy is applied to an L2 ATM interface before a valid policy is applied:

Remove existing Service-policy CBR before applying new Service-policy egress

Conditions: This symptom is observed only on a Cisco router that is configured with a secondary RP and ATM L2VPNs that function in the VP mode.

Workaround: There is no workaround.

- CSCeh50638

Symptoms: A 4-port Gigabit Ethernet ISE line card may crash.

Conditions: This symptom is observed on a Cisco 12000 series that is configured for multicast traffic.

Workaround: There is no workaround.

- CSCeh51720

Symptoms: When the router is configured with a new area, the links that are configured for TE are not flooded in the new area.

Conditions: This symptom is observed when you configure an area by entering the **mpls traffic-eng area number** command as part of the router OSPF configuration.

Workaround: There is no workaround.

- CSCeh52241

Symptoms: Fault recovery may fail to recover memory contents on ECC faults for certain FSRAM memory locations.

Conditions: This symptom is rarely observed on a Cisco 12000 series.

Workaround: There is no workaround.

- CSCeh53373

Symptoms: A TE tunnel does not come up.

Conditions: This symptom is observed in an MPLS TE interarea configuration.

Workaround: There is no workaround.

- CSCeh54615

Symptoms: LSPs that support AToM circuits may fail to come up.

Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS software image that includes the fix for DDTS ID CSCeg74562. A list of the affected releases can be found at <http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg74562>. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

Workaround: There is no workaround.

- CSCeh55841

Symptoms: When you remove one CSC or one SFC, all traffic stops because there is insufficient fabric bandwidth. However, when you re-insert the CSC or SFC, all interfaces remain down.

Conditions: This symptom is observed on a Cisco 12000 series.

Workaround: Reload the router.

- CSCeh56377

Symptoms: VRF RP mapping continues to toggle between the RPs of two CE routers.

Conditions: This symptom is observed when a Cisco 12000 series that functions as a PE router is located between the two CE routers.

Workaround: Reset the PIM neighbor for the CE router that has the lower IP address of the two CE routers.

- CSCeh57695

Symptoms: A PE router that is configured for MPLS VPN—Carrier Supporting Carrier drops decapsulation traffic in the direction of a CE router. Encapsulation traffic works fine and is not affected.

Conditions: This symptom is observed when MPLS VPN--Carrier Supporting Carrier is configured with Label Distribution Protocol (LDP) as the protocol between the PE router and a CE router. In some circumstances such as a BGP peer flap or a route flap, LDP may free the local label that is allocated by BGP while BGP still uses the label. The same label may be allocated later for a different prefix, causing multiple prefixes to use the same local label, and, in turn, causing connectivity for the affected prefixes to fail.

Workaround: There is no workaround.

- CSCeh58983

Symptoms: When a router is reloaded with a scaled L2VPN configuration, the secondary RP may reload unexpectedly because of a “BFRP HA Chkpt send” failure.

Conditions: This symptom is observed on a Cisco 12000 series that runs the c12kprp-p-mz image of a Cisco IOS interim release for Release 12.0(31)S.

Workaround: There is no workaround.

- CSCeh59116

Symptoms: When an HA switchover occurs in an L2VPN scaled configuration, some of the subinterfaces on a 4-port Gigabit Ethernet ISE line card may use the incorrect MAC address for the destination MAC address, which you can see in the output of the **show adjacency detail** command.

Conditions: This symptom is observed on a Cisco 12000 series that runs the c12kprp-p-mz image of a Cisco IOS interim release for Release 12.0(31)S.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected subinterfaces.

- CSCeh59410

Symptoms: When traffic flows from an Engine 6 line card to a link-bundle interface (a POS interface or PortChannel interface), the Engine 6 line card cannot load-balance traffic between the physical ports that are part of the link bundle. This situation may cause traffic to be lost and may prevent the interface from being used to its full capacity.

Conditions: This symptom is observed on a Cisco 12000 series that runs a Cisco IOS interim release of Release 12.0(31)S and occurs for IP-to-IP traffic and when MPLS is globally disabled

Workaround: Enable MPLS globally (default).

- CSCeh59452

Symptoms: An RP switchover may cause a 6-port channelized T3 Engine 0 line card to fail.

Conditions: This symptom is observed on a Cisco 12000 series that runs a Cisco IOS interim release for Release 12.0(31)S, that has two PRPs, and that functions in RPR+ redundancy mode.

Workaround: There is no workaround.

- CSCeh60185

Symptoms: An Engine 4 plus (E4+) line card that functions in an IP-to-tag switching scenario may generate “TX192-3-PAM_MODULE” and “%TX192-3-PAM_PIM” error messages and tracebacks or may crash.

Conditions: This symptom is observed on a Cisco 12000 series when the ingress interface is an Engine 2 line card that has an input ACL and when an external LDP flap occurs that affects the Engine 4+ line card.

Workaround: There is no workaround.

- CSCeh61467

This caveat consists of the two symptoms, two conditions, and two workarounds:

1. Symptom 1: After you have disabled MVPN on a VRF interface, the CPU use for the PIM process increases to 99 or 100 percent and remains at that level.

Condition 1: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB, Release 12.2SX, or a release that is based on these releases. The symptom may also occur in other releases.

Workaround 1: Before you disable MVPN on the VRF interface, enable and then disable multicast routing by entering the **ip multicast-routing vrf vrf-name** global configuration command followed by the **no ip multicast-routing vrf vrf-name** global configuration command.

2. Symptom 2: A router that functions under stress and that is configured with a VRF interface may crash when an MDT group is removed from a remote PE router.

Condition 2: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB, Release 12.2SX, or a release that is based on these releases, and occurs only when there are frequent link flaps or other multicast topology changes that affect the VRF interface. The symptom may also occur in other releases.

Workaround 2: There is no workaround.

- CSCeh62351

Symptoms: A router or line card may reload when you enter any of the following commands:

On a Cisco 7304:

- **show tech-support** command.
- **show hw-module subslot all status** command.
- **show hw-module subslot slot-number/subslot-number status** command.

On a Cisco 7600 series or Cisco 12000 series:

- **show tech-support** command.
- **show hw-module subslot all status** command.
- **show hw-module subslot subslot-number status** command.

Conditions: This symptom is observed when you enter above-mentioned commands on the console of a Cisco 7304 or on the console of a line card on a Cisco 7600 series or Cisco 12000 series when these routers are configured with any of the following SPAs (some SPAs are specific to the Cisco 7304 and some to the Cisco 12000 series):

- 2-port Gigabit Ethernet SPA
- 4-port FE SPA
- CT3 SPA
- T1/E1 SPA
- T3/E3 SPA

Workaround: There is no workaround.

- CSCeh64632

Symptoms: After a Route Processor or line card has reloaded, the queue limit that is set for the class default is not properly programmed.

Conditions: This symptom is observed on a Cisco 12000 series 1-port channelized OC-12/STM-4 (DS1/E1) ISE line card that has an egress policy applied to a serial interface.

Workaround: There is no workaround.

- CSCeh65748

Symptoms: A Engine 3 ISE line card may not properly handle incoming bad IP packets but may generate a traceback and a transient error message:

```
%GSR-3-INTPROC: Process Traceback= 400E10B4 400FBA2C
-Traceback= 4047917C 405E5274 400F4B58
%EE48-3-BM_ERRS: FrFab BM SOP error 40000
%EE48-3-BM_ERR_DECODE: FrFab SOP macsopi_bhdr_pkt_len_zero_err

%GSR-3-INTPROC: Process Traceback= 400E1090 400FBA2C
-Traceback= 4047917C 405E5274 400F4B58
%LC-4-ERRRECOVER: Corrected a transient error on line card.
```

The line card may also crash.

Conditions: These symptoms are observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(26)S1 or Release 12.0(26)S5a.

Workaround: There is no workaround.

- CSCeh66946

Symptoms: An interface stops traversing traffic through an Engine 6 2xOC192 POS line card.

Conditions: This symptom occurs when AToM is configured on an Engine 6 2xOC192 line card (facing the edge).

Workaround: There is no workaround.

- CSCeh70093

Symptoms: The **no** form of a configuration command such as the **no shutdown** controller configuration command may not be properly synchronized to the standby RP.

Conditions: This symptom is observed on a Cisco 12000 series that functions in SSO redundancy mode and that is configured with a 6-port channelized T3 line card. When you enter the **no shutdown** controller configuration command on the T3 controller of the 6-port channelized T3 line card, the **no shutdown** configuration does not synchronize to the standby RP, and after an SSO switchover has occurred, the T3 controller remains in the adminDown state on the newly active RP.

Workaround: Manually enter **no shutdown** controller configuration command on the T3 controller after the RP switchover has occurred.

- CSCeh73978

Symptoms: When configuring service policies on any interface, the console erroneously displays a message indicating that Rate Limit and Policing can only be configured together on 4 port ISE Ethernet cards. More importantly, it prevents the service policy from being applied to the interface.

Conditions: This symptom has been observed on startup or anytime the configuration is entered.

Workaround: There is no workaround.

- CSCeh76209

Symptoms: When Policy Based Routing (PBR) is configured with the **set interface** command, packets continue to be forwarded to an interface when that went down, causing packets to be dropped. When the **ip local policy route-map** command is enabled, all locally-generated packets are impacted.

Conditions: This symptom is observed on a Cisco router and only applies to packets that require process-switching.

Workaround: Do not enter the **set interface** command. Rather, enter the **set ip next-hop** command.

- CSCeh78918

Symptoms: When a line card has reloaded because you reloaded the router, the line card crashed, or you entered a command to reload the line card, the following message may appear on the console:

```
%MDS-2-RP: MDFS is disabled on some line card(s). Use "show ip mds stats linecard" to view status and "clear ip mds linecard" to reset.
```

This message may be generated because MDFS is erroneously disabled on the reloaded line card. Erroneous disabling of MDFS may unnecessarily extend network convergence time.

Conditions: This symptom is observed on a distributed router or switch such as a Cisco Catalyst 6000 series, Cisco 7500 series, Cisco 7600 series, Cisco 10000 series, and Cisco 12000 series. The symptom occurs when the router has the **ip multicast-routing distributed** command enabled for any VRF and when a line card is reloaded more than 50 seconds into the 60-second MDFS flow-control period.

Workaround: The symptom corrects itself after 60 seconds. Alternatively, you can enter the **clear ip mds linecard slot number** command.

- CSCeh82971

Symptoms: A Cisco router crashes when performing an FPD image upgrade operation.

Conditions: This symptom can occur if the sending of the FPD image from RP to a line card fails because the target card is reloaded during this time window.

Workaround: Do not reload or physically remove the target upgrade line card when performing an FPD image upgrade.

- CSCeh84320

Symptoms: The subinterface on the modular GE/FE card stops forwarding.

Conditions: This symptom occurs whenever the operator enters sub-interface mode with an xconnect statement on the EPA-GE/FE-BBRD fixed port on the modular GE/FE card.

Workaround: While in the sub-interface mode, the operator can enter a **shutdown** command followed by a **no shutdown** command which allows the subinterface to resume forwarding.

Each time the operator enters the sub-interface on the fixed port, the workaround will need to be applied.

- CSCeh84740
Symptoms: An RPR+ switchover may cause a VIP or line card to pause indefinitely.
Conditions: This symptom is observed when a high load of traffic passes through interfaces of a VIP or line card when these interfaces are configured for QoS.
Workaround: There is no workaround.
- CSCeh90984
Symptoms: When you enter the **clear cef linecard** command, CEF may be disabled on a POS ISE line card and does not recover by itself.
Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S3.
Workaround: Reload the line card.
- CSCeh91772
Symptoms: If an existing file is extended, an ATA file system may become corrupted. When this situation occurs, the output of the **dir** command or of a **show** command does not list the files because the files are corrupted.
Conditions: This symptom is observed when you enter any command that extends a file such as the **show interfaces ethernet | append disk0:file** command.
Workaround: Do not enter a command that extends a file.
- CSCeh97080
Symptoms: When Multiprotocol Label Switching (MPLS) is enabled on a router, one or more LDP sessions may be disrupted during periods of extremely high CPU use.
Conditions: This symptom is observed when the CPU use of the router temporarily increases to more than 90 percent for several tens of seconds and when one or more high-priority processes are frequently active but do not necessarily use many CPU cycles.
For example, high CPU use may occur when a peer router is reloaded or when an interface with several hundreds of numbered IP subinterfaces comes up, which causes many processing changes on the router because of the “Tagcon Addr” process.
On a Cisco 12000 series, high CPU use may occur because of the “Fabric ping” high-priority process, which is frequently active.
Other high-priority processes may also cause the symptom to occur.
Workaround: To increase the length of the hello adjacency holdtimes, enter the **mpls ldp discovery hello holdtime** command on the affected router. You may need to enter this command on all platforms in the network in order to provide full protection.
- CSCeh97671
Symptoms: When an RP switchover occurs, the standby RP crashes, causing the switchover downtime to be longer than expected and traffic to be affected.
Conditions: This symptom is observed on a Cisco 12000 series that is configured for HA when you perform an RP switchover, when the active RP runs Cisco IOS Release 12.0(28)S4, and when the standby RP runs a Cisco IOS interim release later than Release 12.0(31)S.
Workaround: There is no workaround.

- CSCeh97760

Symptoms: In the outputs of the **show ip psa-cef** and **show ip cef** commands for an Engine 2 ingress line card, the “Local OutputQ (Unicast)” information may point to another and incorrect slot than the slot that the global CEF table points to.

When this symptom occurs, packets that are destined for these specific IP address are dropped.

Conditions: This symptom is observed on a Cisco 12000 series when an Engine 2 line card is used as an ingress line card for traffic that is directed to a default route.

Workaround: Enter the **clear ip route 0.0.0.0** or **clear ip route *** command.

- CSCeh97829

Symptoms: An RP may crash continuously when you reload all the line cards in a dual-RP router that has the redundancy mode is set to SSO.

Conditions: This symptom is observed on a Cisco 12000 series that is configured with two GRPs or two PRPs that are configured for SSO and occurs only when a 1-port channelized OC-48 ISE line card, a 4-port channelized OC-12 ISE line card, or 16-port channelized OC-3 ISE line card is present in the router.

Workaround: Set the redundancy mode to RPR or RPR+.

- CSCei00027

Symptoms: On a channelized OC-48 ISE line card with APS configured, a “Signal Failure” condition remains after the line card has been reloaded or after you enter the **shutdown** command followed by the **no shutdown** command.

Conditions: This symptom is observed on a Cisco 12000 series and affects only a channelized OC-48 ISE line card with an APS configuration.

Workaround: There is no workaround.

- CSCei01644

Symptoms: A 3-port Gigabit Ethernet (3GE-GBIC-SC) line card that is configured for Fast-Path Multicast Forwarding may reset when receiving specific packets. However, it is not necessary that the line card will crash all times. The resulting action on these packets could result in a simple drop as well.

Conditions: This symptom is observed on a Cisco 12000 series when a packet with an IP destination address from the reserved multicast range (224.0.0.xxx) and a TTL larger than 1 is received on the 3GE-GBIC-SC line card and when multicast hardware acceleration is enabled.

Normally, the TTL should be 1 if the destination address is part of the reserved multicast range.

Workaround: Enter the **no hw-module slot slot-number ip multicast hw-accelerate source-table size 16 offset 0** command.

- CSCei03674

Symptoms: Class-default counters (that is, the total number of packets) do not increment.

Conditions: This symptom is observed on a Cisco router when a class map matches an OAM that is applied to a policy.

Workaround: There is no workaround.

- CSCei04350

Symptoms: MVPN PIM neighbors that are associated with both a 1-port channelized OC-48 ISE line card and a 1-port channelized OC-12 (DS1) ISE line card bounce when you perform a microcode-reload of a 1-port channelized OC-12 (DS1) ISE line card.

Conditions: This symptom is observed on a Cisco 12000 series.

Workaround: There is no workaround.

- CSCei04912

Symptoms: If a 4-port Engine 3 Gigabit Ethernet (GE) line card is fast reroute (FRR) headend, and only the RX cable is pulled out, convergence time is greater than 50ms.

Conditions: This symptom occurs when the 4-port Engine 3 GE line card is FRR headend, and only the RX cable is pulled out.

Workaround: There is no workaround.

- CSCei05246

Symptoms: After an OIR of a PA-MC-E3 port adaptor that is installed in a VIP6-80, the serial interfaces do not transmit. The message “not transmitting” is generated, followed by “output frozen.” After these messages, a Cbus Complex occurs.

Conditions: This symptom is observed on a Cisco 7500 series.

Workaround: There is no workaround.

- CSCei05312

Symptoms: An EERP-3-INVALID_LAYER error message may be generated followed by continuous tracebacks that flood the screen, causing some tracebacks to be dropped.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS 12.0(31)S and that is configured with an ATM VC and VP when a policy map of the following type is attached and when OAM traffic is sent on the VC or VP:

```
policy foo
    class oam
        set mpls exp 6
    class class-default
        police xyz cps conform-action transmit exceed-action drop
        service child
    policy child
        class clp0
            police abc cps conform-action transmit exceed-action drop
```

Workaround: Remove the above-mentioned policy from the VP or VC.

First Alternate Workaround: Stop sending the OAM traffic.

Second Alternate Workaround: Configure an alternative policy such as the following one:

```
policy foo
    class class-default
        police xyz
        service child
    policy child
        class oam
            set ...
        class clp
            set ...
        class class-default
            police xyz cps
```


- CSCei07556

Symptoms: The PPP protocols flap on a 64K-port of an interface of a 1-port channelized OC-12/STM-4 (DS1/E1) ISE line card that is configured for CoS and that is congested.

Conditions: This symptom is observed when two Cisco 12000 series are connected back-to-back, when the routers are connected via 1-port channelized OC-12/STM-4 (DS1/E1) ISE line cards, and when you send real-time traffic.

Workaround: Change the QoS output policy to prevent traffic from being for longer than 10 seconds and enable keepalive packets to time out.

Further Problem Description: The symptom does not occur when you do not send real-time traffic.

- CSCei07805

Symptoms: When a router has a large VRF configuration and a lot of routing information, the following error messages may be generated during an SSO switchover:

```
%FIB-3-FIBDISABLE: Fatal error, slot/cpu 5/0: keepalive failure
```

The following CPUHOG error message and traceback may also be generated:

```
%SYS-3-CPUHOG: Task is running for (2000)msecs, more than (2000) msecs  
(272/145),process = IPC LC Message Handler.  
-Traceback= 40EAF5D8 411DBE94 411DBFB8 411DC5D0 411DEFEC 411DEE90 411E0200 41093100  
410932B8
```

After the FIBDISABLE error messages has been generated, the router may no longer function properly.

Conditions: This symptom is observed on a Cisco 7600 series but is platform-independent.

Workaround: There is no workaround.

- CSCei07946

Symptoms: When the active rate for a destination PE router is evenly distributed at 4 pps for 20 flows and the active rate for a destination CE router is evenly distributed at 4 pps for 19 flows, one flow is reported at twice that rate (that is, 8 pps).

Conditions: This symptom is observed on a Cisco 12000 series that functions in a MVPN VRF-Lite environment with 20 multicast streams that have a single sustained cell rate (SCR) and that have the pps rate evenly distributed across all streams.

Workaround: There is no workaround.

- CSCei08381

Symptoms: Engine 3 and Engine 5 line cards in a Cisco 12000 series may fail continuously.

Conditions: This symptom is observed on a Cisco 12000 series that runs a Cisco IOS interim release for Release 12.0(32)S when control-plane policing is configured on the line cards in the router.

Workaround: There is no workaround.

- CSCei08472

Symptoms: The following error message is displayed:

```
Router(config)#policy-map foo Router(config-pmap)#class match_precl  
Router(config-pmap-c)#band per 2 Service-policy is not supported on interface  
Multilink100.
```

Conditions: This symptom occurs when a service policy that is attached to a multilink interface with no members is modified.

Workaround: There is no workaround.

- CSCei08823

Symptoms: When a ToFab FCRAM single-bit error (SBE) occurs on an Engine 5 line card, the following error message is generated, and the line card resets:

```
Tofab BMA has lost a command
```

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S and occurs only on an Engine 5 line card.

Workaround: There is no workaround.

- CSCei09755

Symptoms: When you remove a multilink bundle by entering the **no ppp multilink** command under a serial link configuration, a serial link that is configured in the multilink bundle remains in the “line protocol down” state and does not recover.

Conditions: This symptom is observed on a Cisco 7600 series that is configured with a SIP1 line card in which a SPA-CT3 is installed and on a Cisco 12000 series that is configured with a SIP-400 or SIP-600 in which a SPA-CT3 is installed.

Workaround: Reload the SPA by entering the **hw-module subslot slot subslot reload** command.

- CSCei09876

Symptoms: A router that is configured for MPLS VPN cannot accept a Route Distinguisher with the value 0:0.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0S or Release 12.4 and that integrates the fix for CSCeh12594. A list of the affected releases can be found at <http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeh12594>. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

Workaround: Use a Route Distinguisher with another value. If this is not an option, there is no workaround.

- CSCei10528

Symptoms: The tunnel interface does not come up when you configure an MPLS TE tunnel for IS-IS.

Conditions: This symptom is observed on a Cisco 12000 series ATM ISE line card that is configured for IS-IS. The symptom does not occur when the line card is configured for OSPF.

Workaround: There is no workaround.

- CSCei12538

Symptoms: Using the **show ssm id** command on a line card after a switchover may crash the line card.

Conditions: This symptom is observed in Cisco IOS Release 12.0(31)S on dual RP platforms that are running high availability (HA). After a switchover, if the **show ssm id** command is issued on a line card, the line card may crash.

Workaround: Do not use the **show ssm id** on a line card.

- CSCei12771

Symptoms: All traffic with a 0 label plus another label is dropped by a 3-port Gigabit Ethernet egress ISE line card.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S.

Workaround: There is no workaround.

- CSCei15701

Symptoms: The active PRP pauses indefinitely after it changes from standby to active.

Conditions: This symptom is observed when the redundant PRPs are configured for RPR+ mode, the router has two APS-protected CHOC12 line cards, the router has mVPNs configured, and the router runs Cisco IOS Release 12.0(28)S3.

Workaround: There is no workaround.

- CSCei18287

Symptoms: When there are some incomplete xconnect configurations or rapid succession of unprovisioning and provisioning of xconnect, memory leaks may be observed on line cards in Segment Switch Manager (SSM).

Conditions: This symptom occurs in Cisco IOS Release 12.0(31)S or later releases.

Workaround: There is no work around.

- CSCei22697

Symptoms: Some MVPN tunnels are mapped to an incorrect VRF forwarding table.

Conditions: This symptom is observed on a Cisco router that is configured for data MDT groups.

Workaround: There is no workaround.

- CSCei24302

Symptoms: When traffic enters an Engine 6 ingress interface and flows in the direction of equal-cost multiple egress interfaces, all traffic is lost.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(27)S5, Release 12.0(28)S3, or Release 12.0(31)S when the traffic destination is present in the routing table as a recursive route (for example, learned via iBGP) and when the router has the IP Source Tracker feature configured. The symptom occurs only when the ingress interface is an interface of an Engine 6 link card and when multiple equal-cost egress interfaces are used.

Workaround: Enter the **clear ip route *** command to enable the traffic to reach its destination.

- CSCei26310

Symptoms: High memory usage, high CPU usage, or both may occur on a router that is configured for Xconnect.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0S or Release 12.2S when one of the following conditions occurs:

- The MFR data plane provisioning fails.
- The PW redundancy feature set is configured and the provisioning of the data plane fails for one of the redundancy members.

There may also be other conditions that cause the symptom to occur.

Workaround: If MFR data plane provisioning fails, there is no workaround. If the PW redundancy feature set is configured, there is a workaround: configure a large value for the “enable” and “disable” timeouts.

- CSCei27448

Symptoms: A router may crash while displaying the output of the **show ip pim mdt bgp** command.

Conditions: This symptom is observed when withdraws for a MDT source group are received by PIM from BGP while you enter the **show ip pim mdt bgp** command.

Workaround: There is no workaround. To reduce the chance of the router crashing, change the *screen-length* argument in the **terminal length screen-length** command to 0. Doing so prevents the router from pausing between multiple output screens. (The default of the *screen-length* argument is 24.)

- CSCei29398

Symptoms: A standby RP crashes when you add or remove classes from a QoS policy or when a policy is applied to one line rather than to multiple lines.

Conditions: This symptom is observed on a Cisco 12000 series but is platform-independent.

Workaround: There is no workaround.

- CSCei30764

Symptoms: A PE router that is configured with many (100 or more) Multicast VRFs (mVRFs) may create multiple MDT tunnels for one mVRF.

Conditions: This symptom is observed when you reload a Cisco router that functions as a PE router and that is configured for MVPN.

Workaround: There is no workaround.

- CSCei31560

Symptoms: When a multilink bundle is configured on a 6-port channelized T3 line card, the delay for traffic in the priority queue may be 12 to 14 milliseconds more than what you would expect.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0S when a multilink protocol such as MFR or MLP is configured and when congestion occurs.

Workaround: There is no workaround.

- CSCei35132

Symptoms: When a link failure occurs between two provider (P) routers, the LSP that is protected via Fast Reroute (FRR) for a primary tunnel and the directed LDP session within the tunnel are fast-rerouted onto an assigned backup tunnel. However, when the backup tunnel goes down, VPN prefixes that are protected by backup TE LSP entries in the LFIB become “Untagged.” This situation causes packet loss for ATOM and L3VPN traffic that uses the link between the P routers as its primary path.

Conditions: These symptoms are observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S, that functions as a P router, and that is connected to another P router via a 4-port OC-3 ISE line card.

The topology is as follows:

```
PE ----- P --- OC-3 --- P ----- PE
```

There are one-hop primary tunnels between every pair of routers that is listed above, and each link is protected by an NHOP backup tunnel LSP.

The symptom occurs when you pull the TX fiber cable from the 4-port OC-3 ISE line card that forms the protected link between the two P routers, when the protected LSP is fast-rerouted onto the backup tunnel, and when the backup tunnel is torn down. One P router may show “Untagged” entries in its LFIB, especially for a loopback interface to a provider edge (PE) router. This situation breaks the forwarding for all of the L2 and L3 VPNs that depend on that PE router.

The symptom is timing-dependent. The symptom does not occur all the time and does not seem to be Cisco 12000 series line card-dependent, nor is it specific to a link between the two P router because the symptom may also occur when you pull the TX fiber cable of a line card that forms the link between a PE router and a P router.

Workaround: There is no workaround.

- CSCei36381

Symptoms: When QOS parameters are changed, traffic does not pass via an L2TPv3 link.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S when QOS or HQoS parameters are changed and affect the traffic flow.

Workaround: Reload the affected line card or reload the router.

- CSCei37227

Symptoms: You cannot link a CoS slot table definition to a line card by entering the **rx-cos-slot** global configuration command. When you attempt to do so, the following error message is generated:

```
% Unknown Cos Queue Group - ToFab-Policy
```

Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of a Cisco IOS interim release later than Release 12.0(31)S.

Workaround: There is no workaround.

- CSCei37523

Symptoms: When you reload all the line cards on a Cisco 12000 series or when you initiate an RP switchover, a %PRP-3-CHP_DESCQ_FULL error message may be generated and some of the line cards may fail.

Conditions: This symptom is observed on a Cisco 12000 series that runs a Cisco IOS interim release later than Release 12.0(31)S when one of the clock and scheduler cards (CSCs) is shut down.

Workaround: Reload the affected line cards.

- CSCei38116

Symptoms: ISE line cards crash when a Cisco 12000 series receives 640,000 multicast streams.

Conditions: This symptom is observed when the memory of the ISE line cards becomes exhausted when the thousands of multicast streams are received.

Workaround: There is no workaround.

- CSCei39383

Symptoms: Interface configuration parameters are not applied to the running configuration after an RPR+ switchover.

Conditions: This symptom is observed intermittently on a Cisco 12000 series that is configured with a 1-port CHOC-48 ISE line card but may also occur with other line cards.

Workaround: Apply the configuration manually to the affected interface.

- CSCei40168

Symptoms: An AToM VC that is configured on a Fast Ethernet or Gigabit Ethernet interface may not be functional and packets that are received on the interface are dropped.

Conditions: This symptom is observed on a Cisco 10720.

Workaround: Reconfigure the **xconnect** command on the affected interface.

Further Problem Description: When the symptom occurs, the output of the **show hardware pxf cpu statistics interface interface-name detail** command shows that the packets that are received on the interface are dropped because of an “mpls undefined port” condition.

- CSCei40506

Symptoms: Performance drops to 90 percent when the “N flag” is set incorrectly for the MDFS process.

Conditions: This symptom is observed on a Cisco 12000 series that is configured for mVPN, that uses an Engine 3 line card for imposition, and that uses an Engine 4+ line card for disposition.

Workaround: Reload the router.
- CSCei40645

Symptoms: When a Gigabit Ethernet (GE) link goes down between two 4-port GE ISE line cards, the link detection mechanism is inconsistent.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S.

Workaround: There is no workaround.
- CSCei41469

Symptoms: The standby PRP crashes when you apply an IPv6 ACL on an interface of an ISE line card.

Conditions: This symptom is observed on a Cisco 12000 series that is configured with redundant PRPs.

Workaround: There is no workaround.
- CSCei48251

Symptoms: A router that is configured for Pseudowire Redundancy may generate the following stack trace:

```
FP: 0x4581CE80[etext(0x42316c92)+0x35061ee], RA: 0x4154B924
[atom_seg_packet_process_send_func(0x4154b81c)+0x108]
FP: 0x4581CEC0[etext(0x42316c92)+0x350622e], RA: 0x4045A87C[sss_switch_pak
(0x4045a5d8)+0x2a4]
FP: 0x4581CF50[etext(0x42316c92)+0x35062be], RA: 0x418CDA98
[ac_vlan_switching_receive_pak_process(0x418cd924)+0x174]
FP: 0x4581CFA0[etext(0x42316c92)+0x350630e], RA: 0x418CC1DC
[ac_switching_receive_pak_process(0x418cbfec)+0x1f0]
FP: 0x4581D008[etext(0x42316c92)+0x3506376], RA: 0x418CC920[acswitch_process
(0x418cc8a4)+0x7c]
```

Conditions: This symptom is observed on a Cisco router that has one AToM and one non-AToM segment.

Workaround: There is no workaround.
- CSCei48635

Symptoms: Multilink Frame Relay (MFR) interfaces that are configured on a channelized T3 SPA continue to flap.

Conditions: This symptom is observed on a Cisco 12000 series when you perform an online insertion and removal (OIR) of the 12000-SIP-400 in which the channelized T3 SPA is installed, or when the router reloads.

Workaround: Enter the **hw-module slot slot-number reload** command.

- CSCei48728

Symptoms: New subinterfaces and duplicate IP addresses are unexpectedly created for member interfaces of a port-channel subinterface.

Conditions: This symptom is observed on a Cisco 12000 series that is configured with dual Route Processors that function in RPR mode when a clock and scheduler card (CSC) is shut down before an RPR switchover occurs.

Workaround: There is no workaround.

- CSCei48972

Symptoms: After a manual switchover occurs in RPR+ mode, a VPN that is configured on a Frame Relay subinterface fails to recover and CEF may be disabled on line cards.

Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of a Cisco IOS interim release for Release 12.0(30)S2.

Workaround: Enter the **hw-module slot slot-number reload** command.

- CSCei49180

Symptoms: A standby RP resets when you add a channel group by entering the **channelized [mode t1 | e1]** command on the controller of a T3 port that had the **no-channelized** command enabled before you made the change.

Conditions: This symptom is observed on a Cisco 12000 series that has two RPs and that is configured with a 4-port channelized T3 to DS0 Shared Port Adapter (SPA) that is installed in a 2.5G ISE SPA Interface Processor (SIP).

Workaround: There is no workaround.

- CSCei51504

Symptoms: When you run an SNMP get or walk on the ifOperStatus object on a 1-port CHOC-12 OC-3 ISE line card, the status for the STS-1 path interface shows down although the channel is up.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S3.

Workaround: There is no workaround.

- CSCei52380

Symptoms: The entry for a tunnel is missing from the mplsOutSegmentTopLabel column of the MPLS-LSR-MIB.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4 when a mibwalk is performed on the mplsOutSegmentTopLabel object. The symptom may also occur in other releases.

Workaround: There is no workaround.

- CSCei54336

Symptoms: An MPLS LER does not impose labels for traffic that follows the default route, causing traffic to be forwarded via IP.

Conditions: This symptom is observed on a Cisco 12000 series when the default route has two equal paths, when the ingress line card is an ISE line card, and when the default router is learned via OSPF. The symptom may also occur for other protocols.

Workaround: Use a single path for the default route. If this is not an option, there is no workaround.

- CSCei58551
Symptoms: A 1-port OC-192 Engine 4+ line card (OC192E/POS) or a Modular GbE Engine 4+ line card (EPA-GE/FE-BBRD with EPA-3GE-SX/LH-LC) may crash when an SSO switchover occurs or when the router reloads.
Conditions: This symptom is observed on a Cisco 12000 series that runs a c12kprp-p-mz image of Cisco IOS Release 12.0(31)S and that has two RPs.
Workaround: There is no workaround.
- CSCei64939
Symptoms: When a service policy is attached to an ATM PVP as an output policy that contains a queue limit, the policy is rejected with the error message “No ATM VC associated with this service policy.”
Conditions: This symptom is observed only for ATM VP connections when a policy is attached as an output policy with a queue limit.
Workaround: There is no workaround.
- CSCei69208
Symptoms: A Cisco router crashes by unexpected exception to CPUvector 300.
Conditions: This symptom is observed on a Cisco 12000 series router.
Workaround: There is no workaround.
- CSCei69875
Symptoms: Hardware multicast forwarding does not function.
Conditions: This symptom is observed on a Cisco 12000 series after you have reloaded the router.
Workaround: Remove and re-apply hardware multicast forwarding.
- CSCei71478
Symptoms: A 4-port GE ISE line card that is configured with 30 or more VLAN subinterfaces may fail.
Conditions: This symptom is observed on a Cisco 12000 series that runs a Cisco IOS release that is later than Release 12.0(31)S. The symptom may also occur on a 5-port GE Engine 5 SPA.
Workaround: There is no workaround.
- CSCei74449
Symptoms: Line cards may enter the WAITRTRY state when the primary CSC is shut down.
Conditions: This symptom is observed only on a Cisco 12008 that runs an interim release for Cisco IOS Release 12.0(32)S when the active RP is installed in slot 2 of the chassis.
Workaround: Ensure that the active RP is not installed in slot 2 of the chassis.
- CSCei75742
Symptoms: MPLS may fail on a router when you reload a Gigabit Ethernet (GE) line card on which Link Bundling is enabled.
Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S or an interim release for Release 12.0(32)S.
Workaround: Re-enable MPLS by entering the **mpls ip** global configuration command.

- CSCei79855

Symptoms: When Cisco IOS software is secured using “secure boot” commands and after formatting the disk, the **show disk** command will not display the secured image and the corresponding configurations in the output.

Conditions: This symptom occurs when securing the Cisco IOS software using the **secure boot-config** and the **secure boot- image** commands and formatting the disk.

Workaround: There is no workaround.

- CSCei83160

Symptoms: PIM neighbors do not recognize each other via a VRF tunnel interface because multicast does not receive MDT updates from BGP. The output of the **show log** command shows the following debug message:

```
%BGP-3-INVALID_MPLS: Invalid MPLS label (3) received in update for prefix
2:55:1111:192.168.31.1/32 from 192.168.31.1
```

Conditions: This symptom is observed on a Cisco router and is not platform-dependent. The symptom occurs when a VRF instance is configured with BGP as the Exterior Gateway Protocol (EGP).

Workaround: There is no workaround.

- CSCei83644

Symptoms: A nondefault configuration becomes lost for a serial interface on a channelized OC-48 ISE line card or on a 4-port OC-12 ISE line card.

Conditions: This symptom is observed on a Cisco 12000 series after you have reloaded the router.

Workaround: There is no workaround.

- CSCei84353

Symptoms: A router crashes when you remove an Embedded Event Manager (EEM) applet.

Conditions: This symptom is observed on a Cisco 12000 series that runs an interim release for Cisco IOS Release 12.0(32)S. This symptom occurs under the rare occasion that the EEM applet is removed while EEM is attempting to trigger the applet for execution.

Workaround: Perform the following three steps:

1. Before you remove the EEM applet, disable EEM applet scheduling by entering the **event manager scheduler applet suspend** command.
2. Remove the applet.
3. After you have removed the applet, re-enable EEM applet scheduling by entering the **no event manager scheduler applet suspend** command.

- CSCei86192

Symptoms: When a buffer leak occurs, the RP crashes because of the starvation of buffers.

Conditions: This symptom is observed on a Cisco 7500 series that has a VIP in which a channelized T1/E1 port adapter is installed and on Cisco 7600 series that has a FlexWAN in which a channelized T1/E1 port adapter is installed.

Workaround: There is no workaround.

- CSCei87923

Symptoms: A policy on a main Ethernet interface does not properly match packets for one of its subinterfaces.

Conditions: This symptom is observed on a Cisco 12000 series Ethernet ISE line card when one of its subinterfaces is configured for Xconnect and has a layer 2 VPN configured and when the following events occur:

- You attach a policy to the subinterface.
- You remove the policy from the subinterface.
- You attach the policy to the main interface.

Workaround: There is no workaround.

- CSCei88040

Symptoms: A Cisco 12000 Engine 3 line card might be affected by a memory leak in the “CEF LC IPC Backg” process that is caused by IPv6 route changes.

If all the line card route memory is consumed, the following error messages might be seen:

```
%SYS-2-MALLOCFAIL: Memory allocation of 65556 bytes failed
from 0x400DCE94, alignment 32
Pool: Processor Free: 533440 Cause: Memory fragmentation
Alternate Pool: None Free: 0 Cause: No Alternate pool
-Process= "CEF LC IPC Background", ipl= 0, pid= 71
-Traceback= 40030CBC 400E22FC 400E6A38 400DCE9C 404ADB0C 404ADD80 4042354C 40425464
4114 4B08 411444AC 411443A4 4114B68C 410ECB6C 410ECEB4 410EDC3C

%EE48-3-IPV6_TCAM_CAPACITY_EXCEEDED: IPv6 pkts will be soft ware switched.
To support more IPv6 routes in hardware:
Get current TCAM usage with: show controllers ISE <slot> tcam
In config mode, reallocate TCAM regions e.g. reallocate NetFlow TCAM to IPv6
hw-module slot <num> tcam carve rx_ipv6_1 <prefix> <v6-percent>
hw-module slot <num> tcam carve rx_top_nf <nf-percent>
Verify with show command that sum of all TCAM regions = 100%
Reload the linecard for the new TCAM carve config to take effect
WARNING: Recarve may affect other input features (ACL,CAR,MQC,Netflow)
```

Doing the recarve, as suggested, will not fix the problem, except that by reloading the line card, the leaked memory will be recovered temporarily.

Conditions: This symptom occurs when continuous IPv6 routes change on an Engine 3 line card.

Workarounds:

[1] Reloading the line card can fix the problem temporarily.

[2] Disabling TCAM IPv6 lookups by emptying the IPv6 TCAM:

```
hw-module slot <slot number> tcam carve RX_IPv6_144b_REGION 128 0
hw-module slot <slot number> tcam carve RX_TOP_NF_REGION 39
microcode reload <slot number>
```

To disable [2], just use the “no” form of the command to get back to the default setting:

```
no hw-module slot <slot number> tcam carve RX_IPv6_144b_REGION 128 0
no hw-module slot <slot number> tcam carve RX_TOP_NF_REGION 39
microcode reload <slot number>
```

The default is 35% for NetFlow (RX_TOP_NF_REGION) and 4% for IPv6 (RX_IPv6_144b_REGION 128).

You can check the current status of the TCAM allocation with:

```
exec slot <slot number> sh controllers tofab alpha tcam carve | i
IPv6_128|Total|Mask|RX_TOP_NF
```

Beware: With this workaround, all IPv6 packets will be process-switched on the line card, so make sure you do not have too much IPv6 traffic, or you will get 100% CPU usage on the line card and probably other problems.

[3] Enable IPv6 BGP Dampening to limit the memory leak:

```
...  
address-family ipv6  
bgp dampening  
...  
exit-address-family
```

Note: The problem was not present in Cisco IOS Release 12.0(30)S.

- CSCei90530

Symptoms: An interface of a clear channel T3/E3 SPA that is installed in a 12000-SIP-400 is in a down state after you have entered the **redundancy force-switchover** command.

Conditions: This symptom is observed on a Cisco 12000 series that is configured with two PRPs that function in RPR+ mode.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface to bring the interface back up.

- CSCei90536

Symptoms: mVPN packets have corrupted encapsulation headers.

Conditions: This symptom is observed on a Cisco 12000 series that has a channelized ISE ingress line card when packets are replicated to a VRF interface on the ingress line card, to a VRF interface on another line card, and to a core interface on a third line card. This symptom occurs only after some redundancy switchovers.

Workaround: Reload the line card.

- CSCei90588

Symptoms: A bad checksum error, bad LLS TV length error, or both are reported on a router that is configured for OSPF and BGP. These protocols or other configured protocols may flap during the errors, and data packets that are sent to the PRP may be lost.

Conditions: These symptoms are observed on a Cisco 12000 series that is configured with a PRP-1 when the following conditions are present:

- OSPF, BGP, and other control protocols are configured with scaled routes and peers.
- Congestion occurs on the PRP-1 because control packets are targeted to the PRP-1 or because other packets are sent to one of the IP addresses of the router and are terminated on the PRP-1. This situation occurs, for example, when IP ping packets are directed towards one of the loopback addresses and are terminated on the PRP-1.

Workaround: There is no workaround.

- CSCei91101

Symptoms: Local switching traffic is dropped from the ToFab queue on an egress port of an 2-port T3/E3 serial shared port adapter (SPA) that is installed in a 2.5G ISE SPA Interface Processor (12000-SIP-400).

Conditions: This symptom is observed on a Cisco 12000 series that functions as a PE router in an L2VPN environment.

Workaround: There is no workaround.

- CSCei93119

Symptoms: CEF may become disabled on an Engine E4+ line card because of a MALLOC failure.

Conditions: This symptom is observed on a Cisco 12000 series when you enter the **no mpls ip** global configuration command immediately followed by the **mpls ip** global configuration command.

Workaround: There is no workaround.
- CSCei94758

Symptoms: After an APS switchover, end-to-end traffic does not recover.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)SA4 and that is configured with redundant PRPs that run in RPR+ mode during a Large Scale Network Test (LSNT). The router has two channelized OC-12 line cards that are configured for APS and that each have 280 DS1 ports, 121 DS0 ports, and 42 MLP groups.

Workaround: There is no workaround.
- CSCei94933

Symptoms: When you reload a Cisco 12000 series, the RP remains stuck for 30 minutes. No traceback or spurious memory access is generated after the parser is released.

Conditions: This symptom is observed on a Cisco 12000 series that runs an interim release for Cisco IOS Release 12.0(32)S when the QoS: Enhancements to Single QoS Policy Definition for a Physical Interface (L3/1C/nD) feature is enabled on a T1 interface that is configured for Frame Relay and that has several Frame Relay subinterfaces. The symptom occurs after the following events:

 1. The MQC policy matches the access control list.
 2. You enter the **match fr-dlei** command.
 3. You save the configuration to NVRAM by entering the **copy running-config startup-config** command.
 4. You reload the router.

Workaround: There is no workaround.
- CSCei95220

Symptoms: When an APS switchover occurs on 1-port channelized ISE line cards, traffic may not recover although the controllers may be in up state. The interfaces may remain indefinitely in the up/down state.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S or an earlier release when a significant amount of traffic is being processed when the APS switchover occurs.

Workaround: There is no workaround. However, the built-in failure detection mechanism detects that the ingress data path is locked up and automatically resets the PLIM of the affected line card.
- CSCej00319

Symptoms: A router that is configured for Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) may crash when LDP is configured or removed from an interface or globally.

Conditions: This symptom is observed when parallel links are present.

Workaround: There is no workaround.

- CSCej00776

Symptoms: When you reload a line card or router and then remove a policy, the output of the **show policy-map interface** command shows that no policy is applied but the output of the **show controller frf queue** command does show that the queues are not fully released. This situation prevents traffic from flowing correctly.

Conditions: This symptom is observed on a Cisco 12000 series that is configured with a Gigabit Ethernet Engine 5 SPA that has an “L3/1C/nD” policy map attached to an interface.

Workaround: After you have removed the policy, reload microcode onto the SPA.

- CSCej01615

Symptoms: On a router that is configured for Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP), the CPU usage may increase considerably for an extended period of time when a large number of label bindings are withdrawn or released at the same time.

Conditions: This symptom is observed on a Cisco router only when LDP (as opposed to TDP) is used and when a large number (more than 250) of LDP neighbors and a large number of IP prefixes become unreachable at the same time.

Workaround: There is no workaround.

- CSCej01743

Symptoms: Traffic drops may occur when traffic is sent over MFR or Frame Relay links.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S1 or a later release and that is configured for software forwarding.

Workaround: There is no workaround.

- CSCej04699

Symptoms: The output of the **show ip hardware-cef tofab prefix** command may display incorrect information for Engine 5 line cards.

Conditions: This symptom is observed on a Cisco 12000 series that functions in a scaled routing environment with more than 100,000 routes.

Workaround: There is no workaround.

- CSCej07539

Symptoms: Multicast traffic does not resume fully after you have removed the active PRP from the router.

Conditions: This symptom is observed on a Cisco 12000 series that runs the c12kprp-p-mz image of Cisco IOS Release 12.0(28)S4 and that is configured with redundant PRPs that function in RPR+ mode. The router has two channelized OC-12 line cards that are configured with mVPNs.

Workaround: There is no workaround.

- CSCej09234

Symptoms: The standby RP on a Cisco 12000 series may fail to come up and crash during initialization. The primary RP may generate the following error message:

```
%MBUS-6-DEADSCDY: Standby RP in slot <x> timed out.
```

Conditions: This symptom is observed only when there is a large number of files for the standby RP on the flash disk (for example, when a 1 GB flash disk is about half full) and when the average file size is also large.

Workaround: Delete files on the flash disk.

- CSCej09368

Symptoms: On an Ethernet over AToM link, an abnormal queue depth may occur for Time-Based WRED and Byte-Based-WRED.

Conditions: This symptom is observed on a Cisco 7500 series but is platform-independent.

Workaround: There is no workaround.

- CSCej10404

Symptoms: Fast Reroute (FRR) fails on a remote provider (P) router, causing packet loss.

Conditions: This symptom is observed on a Cisco 12000 series that functions as a P router in the following topology:

- One P router (P1) connects to another P router (P10) via a primary tunnel that is configured on a 1-port 10-Gigabit Ethernet Engine 5 SPA. (P10 functions as the tunnel head-end.)
- There is a backup next-hop (NHOP) FRR protection tunnel via an LSP path between P1 and P10.
- P1 connects also to another P router (P2) that connects to yet another P router (P3), that, in turn, connects to P10, forming a second backup NHOP FRR protection tunnel via an LSP path.

When the link between P1 and P10 breaks at P1, the secondary backup tunnel does not come up immediately, causing packet loss of around 200 ms (about 90 percentile) when the link goes down and 5 seconds when the link finally comes up again.

Workaround: Enter the **mpls traffic-eng topology holddown sigerr 0** command on the affected tunnel head-end (P10) to prevent the backup LSP from being hold down.

Further Problem Description: This symptom is only observed with 1-port 10-Gigabit Ethernet Engine 5 SPAs.

- CSCej14847

Symptoms: Auto-RP messages from a CE router are lost.

Conditions: This symptom is observed when you enter the **clear ip mroute *** on a connected PE router. The messages do not recover by themselves.

Workaround: To restart Auto-RP messages, enter the **clear ip mds linecard** command.

Alternate Workaround: To restart Auto-RP messages, debug the VRF Auto-RP by entering the **debug ip pim vrf vrf-name auto-rp**.

- CSCej15181

Symptoms: A Cisco 12000 series may crash when 1000 pseudowires are configured and one PVP is configured with an existing VCID.

Conditions: This symptom is observed in a L2VPN environment that is configured with 1000 pseudowires when a new configuration overwrites the old configuration with different VCIDs but one of the PVPs has the same VCID as a VCID in the old configuration.

Workaround: There is no workaround.

- CSCej15682

Symptoms: When multicast traffic is being sourced from different sources, and one of the sources is removed, the **show ip mroute vrf** command for the VRFs still shows that source as active.

Conditions: This symptom is observed when a source is no longer active when using the **show ip mroute vrf** command.

Workaround: There is no workaround.

- CSCej15698

Symptoms: The output of the **show ip mroute vrf vrf-name active** command shows an incorrect entry or rate for decapsulated traffic.

Conditions: This symptom is observed on a Cisco 12000 series that is configured for mVPN.

Workaround: There is no workaround.

- CSCej15940

Symptoms: The Queue Manager may not converge on a 4-port OC-12 ATM ISE line card or a 1-port channelized OC-12 ISE line card, and tracebacks may be generated.

Conditions: This symptom is observed on a Cisco 12000 series that runs the c12kprp-p-mz image and occurs after the router has reloaded.

Workaround: There is no workaround.

- CSCej16004

Symptoms: An MTU change on a multilink bundle interface takes no effect for SPA interfaces. This situation may cause the traffic to be dropped.

Conditions: This symptom is observed on a Cisco 12000 series when you change the MTU on a multilink bundle interface and when you change the traffic generation accordingly.

Workaround: There is no workaround.

- CSCej20986

Symptoms: An Engine 4 ingress line card may enter an incorrect carving state in which it sends all packets that are larger than 608 bytes to the buffer size pool (freeq) of the wrong egress line card, causing all packets that are larger than 608 bytes to be dropped. The symptom is especially noticeable when the egress line card is an Engine 2 line card.

Conditions: This symptom is observed rarely on a Cisco 12000 series.

Workaround: Reload the Engine 4 ingress line card.

- CSCej22910

Symptoms: Multicast traffic does not reach a CE router that is connected via static IGMP joins to a PE router.

Conditions: This symptom is observed when the following conditions are present:

- Traffic from the PE router that performs encapsulation flows towards the CE router.
- The PE router that performs decapsulation has an egress line card with one interface connected to the core of the network and another interface connected to the edge of the network.
- The PE router that performs decapsulation has static joins that are configured for Source Specific Multicast (SSM).

Workaround: There is no workaround.

- CSCej23284

Symptoms: In an ATM L2VPN configuration, the protocol of some ATM interfaces on a customer edge (CE) router may be in the DOWN state, causing the corresponding PVCs to be in the DOWN state too.

Conditions: This symptom is observed rarely when an RP switchover occurs on the connected provider edge (PE) router.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected ATM interfaces to enable the PVCs to enter the UP state.

- CSCej24169

Symptoms: High CPU usage occurs on an Engine 6 line card that processes multicast traffic.

Conditions: This symptom is observed on a Cisco 12000 series when the Engine 6 line card is an ingress line card that processes SSM multicast traffic.

Workaround: Lower the traffic rate, configure a mode other than SSM, or replace the Engine 6 line card with an Engine 4 line card.

- CSCej27978

Symptoms: A CE router that is configured for VRFLite does not receive Auto-RP mappings.

Conditions: This symptom is observed when MDS is enabled on the multilink interface that connects the CE router and the PE router.

Workaround: Configure process switching on the multilink interface that connects the CE router and the PE router by entering the **no ip mroute-cache** interface configuration command.

- CSCej32588

Symptoms: An interface of an Engine 6 line card is no longer shut down after an RP switchover occurs.

Conditions: This symptom is observed on a Cisco 12000 series when the following events occur:

1. The interface of the Engine 6 line card is configured with the **no shutdown** interface configuration command in the startup configuration.
2. The router is reloaded and you verify that the interface comes up.
3. You enter the **shutdown** interface configuration command on the interface.
4. You enter the **write memory** command.
5. You enter the **redundancy force** command.

After the new RP comes up, the interface appears no longer shut down and the interface comes up again.

Workaround: After you have entered the **shutdown** interface configuration command on the interface followed by the **write memory** command, reload the router.

- CSCej35344

Symptoms: A multicast group takes a long time to converge on an Engine 6 line card. The output of the **show ip mroute** command shows the multicast group but it does not pass traffic for several minutes. After 8 to 10 minutes, the multicast group passes traffic. The output of the **show ip hardware-mds spd** command shows hardware SPD entries for the multicast group, but the output of the **show ip mds spd** command does not show any software SPD entries for the same multicast group.

Conditions: This symptom is observed on a Cisco 12000 series when traffic from many multicast groups enters the line card before the multicast group Mstate is present, triggering the creation of many SPD entries.

Workaround: Wait for 10 minutes for the extra hardware SPD entries to be cleared up.

- CSCej35650

Symptoms: A deny option does not drop the packets that it is supposed to drop.

Conditions: This symptom is observed on a Cisco 12000 series after you have configured a deny option for an ACL.

Workaround: There is no workaround.

- CSCej36581

Symptoms: When you reload a SIP-600, the following error message is generated:

```
-Process= "CHOCx PRO SPA download channel-group to LC", ipl= 0, pid= 201
```

Conditions: This symptom is observed on a Cisco 12000 series when you reload a SIP-600 in which two channelized OC-3 SPAs are installed (one in bay 2 and one in bay 3).

Workaround: Do not reload the SIP-600.

- CSCej40549

Symptoms: A primary SR-APS physical interface may flap for several minutes in a scaled configuration with 1000 VCs that are configured while the router boots.

Conditions: This symptom is observed on a Cisco 12000 series that runs the c12kprp-p-mz image, that is configured with a 4-port OC-3 ATM ISE line card or 4-port OC-12 ATM ISE line card, and that has SR-APS enabled.

Workaround: There is no workaround.

- CSCej42144

Symptoms: A service policy on an Engine 4 + or Engine 6 line card is incorrectly rejected with the following error message:

```
%E4P and E6 LC requires to configure POLICE and SET %command in every class if either of these two commands %is configured in class-default class
```

This situation occurs when a **set** command is used in all classes.

Conditions: This symptom is observed on a Cisco 12410 that runs Cisco IOS Release 12.0(28)S3, that is configured with dual Performance Route Processors (PRP-1s) that operate in SSO mode, and that has multiple E4+ and/or Engine 6 line cards.

Workaround: There is no workaround.

- CSCej42935

Symptoms: Data corruption may occur on a disk when directory entries are read by more than one process simultaneously.

Conditions: This symptom is observed on a Cisco platform that has an ATA file system when, for example, the **dir disk0:** command is entered on one vty connection and simultaneously, and for the same disk, the **copy disk0:** command is entered on another vty connection.

Workaround: There is no workaround.

- CSCej43126

Symptoms: When you reload a 1-port channelized OC-12 ISE line card, all traffic over the line card may be dropped, and an error message and traceback similar to the following may be generated:

```
%IPCGRP-3-SYSCALL: System call for command 14 (slot7/0) : ipc_send_rpc_blocked  
timed-out (Cause: timeout)  
-Traceback= 1F9F20 1FA028 491DC4 49291C 492D08 2E17EC
```

Conditions: This symptom is observed on a Cisco 12000 series that runs an interim release for Cisco IOS Release 12.0(32)S and that functions in a scaled configuration.

Workaround: Reload the router. If this is not an option, there is no workaround.

- CSCej44769

Symptoms: When you reload a router, the secondary line card in an SR-APS configuration may stay in the “STRTIOS” state for about 20 minutes and then reset to reach the “IOS RUN” state.

Conditions: This symptom is observed on 4-port OC-12 line card that is installed in a Cisco 12000 series and that is configured for SR-APS. The symptom may also occur with an OC-3 ATM ISE line card.

Workaround: There is no workaround.

- CSCej50227

Symptoms: The following error message is generated on a channelized OC-12 ISE line card and traffic is lost:

```
%EE48-3-ALPHA_MCAST: Can't assign new hw_mdb - (S,G)=
```

Conditions: This symptom is observed on a Cisco 12000 series that functions in an MVPN configuration, that has MDFS disabled, that has an Engine 4 Plus line card facing the core of the network, and that has a channelized OC-12 ISE line card facing the edge of the network.

Workaround: There is no workaround.

- CSCej56274

Symptoms: A router or a VIP crashes during the hqf_dp_normalize_class_weights process.

Conditions: This symptom is observed on a Cisco router that is configured for Low Latency Queuing (LLQ).

Workaround: There is no workaround.

- CSCej57949

Symptoms: When you change the Cisco IOS software image from any release to a release later than Release 12.0(27)S2, the redundancy mode is unexpectedly changed from SSO or RPR+ to RPR.

For example, the symptom occurs in the following situations:

- From Release 12.0(26)S4 to Release 12.0(31)S
- From Release 12.0(29)S to Release 12.0(31)S
- From Release 12.0(31)S to Release 12.0(28)S

Conditions: This symptom is observed on a Cisco 7500 series. The symptom does not occur when you change the Cisco IOS software image from any release to a release earlier than Release 12.0(27)S2. For example, the symptom occurs in the following situations:

- From Release 12.0(31)S1 to Release 12.0(26)S4
- From Release 12.0(27)S to Release 12.0(25)S

Workaround: After you have changed the Cisco IOS release, manually change the redundancy mode back from RPR to SSO or RPR+.

- CSCej59084

Symptoms: CEF errors occur when the protection line card is reset, a GRP switchover occurs, or the router is reloaded.

Conditions: This symptom is observed on a Cisco 12000 series that has line card redundancy configured on ATM ISE line cards when you shut down the primary line card of the redundancy pair.

Workaround: Do not shut down the primary line card.

- CSCej67291

Symptoms: A secondary RP does not boot in SSO redundancy mode.

Conditions: This symptom is observed on a Cisco 12000 series.

Workaround: There is no workaround.

- CSCej69557

Symptoms: After you reload a PE router that functions in an MVPN topology and that is configured for sparse mode and Auto-RP, the router may not learn the Auto-RP that is advertised by both a local and remote CE router, preventing traffic from resuming to flow.

Conditions: This symptom is observed on a Cisco 12000 series that runs an interim release for Cisco IOS Release 12.0(32)S and that functions as a PE router. The symptom may also occur in other releases of Release 12.0S.

Workaround: Enter the **clear ip mds line** command.

- CSCej76395

Symptoms: A Layer 2 Protocol Tunnel (L2PT) command does not function when the core-facing line card is an ISE line card. This situation causes the protocol address to be transferred as it is on the pseudowire.

Conditions: This symptom is observed on a Cisco 12000 series when you enter the **l2protocol {cdplstplvtp} tunnel** command on an interface of the core-facing ISE line card.

Workaround: There is no workaround.

- CSCej82265

Symptoms: An MPLS TDP peer is down.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S3 and that has the **mpls ldp protocol tdp** command configured on the interface on which TDP peering cannot be established. The peer router has the **mpls ldp protocol both** command configured.

Workaround: Enter the **mpls ldp protocol tdp** command on the peer router. Note that this workaround may not be plausible for routers that run a legacy Cisco IOS software that only supports TDP.

- CSCej86175

Symptoms: In a multicast VPN (MVPN) environment, when a Stateful Switchover (SSO) occurs on a PE router, the multicast traffic in the MVRF does not recover because the neighboring PE router fails to re-establish its PIM neighbor relationship. Note that the symptom does not occur for unicast traffic.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S2 or an interim release for Release 12.0(32)S and that functions as a PE router (PE1) in the following topology:

```
multicast origination --> PE2 --> PE1 --> CE1 --> multicast termination
```

When an SSO occurs on PE1, PE2 does not re-establish its PIM neighbor relationship with PE1 in the MVRF. PE1 and PE2 are global PIM neighbors.

Workaround: Reload PE1.

Further Problem Description: When the symptom occurs, PE1 still shows PE2 as its PIM neighbor in the MVRF. Clearing the multicast route in the MVRF does not help to resolve this issue.

- CSCek08638

Symptoms: Data traffic that is received by a provider edge (PE) router on an Ethernet port may not be forwarded over an L2TPv3 tunnel.

Conditions: This symptom is observed on a Cisco 12000 series when the line card that faces the customer edge (CE) router is one of the following line cards:

- 8-port Fast Ethernet, 100BASE-FX line card (8FE-FX-SC-B)
- 8-port Fast Ethernet, 100BASE-TX line card (8FE-TX-RJ45-B)
- 1-port Gigabit Ethernet line card (GE-GBIC-SC-B)

Workaround: There is no workaround.

- CSCek17360

Symptoms: When you enable IPv6 on a 4-port GE ISE line card, the line card crashes when it processes Virtual Private LAN Services (VPLS) traffic.

Conditions: This symptom is observed on a Cisco 12000 series when the 4-port GE ISE line card faces the VPLS core.

Workaround: Stop the VPLS traffic. If this is not an option, there is no workaround.

- CSCek24344

Symptoms: When 336 MLP bundles with one link per bundle are configured on four 1-port channelized STM-1/OC-3 Engine 5 SPAs, the following traceback and error messages are generated when you reload one of the Engine 5 SPAs:

```
-Traceback= 406A2188 406A3670 406AA4E8 40339B28 4033C1D0 4033C374 40158D78 40159758
eelc_config_intf_tx_q(): EE_QM_QOS_INTERNAL_ERRORarg=3

%SPA_PLIM-3-HEARTBEAT: Subslot 0 has experienced an heartbeat failure Current
Sequence 14 received Sequence 8 Time since last keep 440ms
```

Conditions: This symptom is observed on a Cisco 12000 series when no traffic is processed on the Engine 5 SPA that is reloaded.

Workaround: There is no workaround.

- CSCek25127

Symptoms: There is no IPv4 BGP MPLS functionality between BGP peers.

Conditions: This symptom is observed on a Cisco 12000 series that is connected to a BGP peer over a link bundle interface.

Workaround: There is no workaround.

- CSCek25442

Symptoms: MFR interfaces may flap on a Cisco 12000 series.

Conditions: This symptom is observed when a high rate of packets are punted to the CPU of the line card that is configured for low-priority Raw Queue (RawQ).

Workaround: Identify the reason for the high rate of packets that are punted to the CPU of the line card and correct the situation.

- CSCin72437

Symptoms: A port adapter in a router or FlexWan module in a switch may crash when an SSO switchover occurs on a Route Processor or Supervisor Engine.

Conditions: This symptom is observed when the port adapter or FlexWan module is configured with a QoS policy.

Workaround: There is no workaround.

- CSCin78176

Symptoms: A Cisco 10000 crashes during per-packet loadbalancing.

Conditions: This symptom is observed on a Cisco 10000 series that runs an interim release for Cisco IOS Release 12.0(30)S when you run multiple tests without cleaning and occurs during the second test after the first test passes. The symptom is platform-independent.

Note: Cleaning comprises of the following steps:

1. Erase all configurations from the router.
2. Load the boot image, load the minimum configuration, and save the configurations.
3. Reload the router with the proper image, and load the proper configurations.

Workaround: There is no workaround. Note that the symptom does not occur when you run the tests with cleaning.

- CSCin78811

Symptoms: If a new multilink bundle is configured, the slave Route Switch Processor (RSP) reloads.

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(24)S6 and that has dual RSPs.

Workaround: There is no workaround.

- CSCin79522

Symptoms: A Cisco router that runs Cisco IOS Release 12.3T may reload when the ATM interfaces are swapped.

Conditions: This symptom is observed when an ATM IMA port adaptor is removed and a PA-A3 port adaptor is inserted in the same slot and when there is at least one PVC configured that has the **inarp** enabled. The symptom may also occur in Release 12.3 or Release 12.4.

Workaround: There is no workaround.

- CSCin79691

Symptoms: QoS information disappears from a FlexWAN module or VIP that is configured with a distributed MFR interface.

Conditions: This symptom is observed after the FlexWAN module or VIP resets or after the interface flaps.

Workaround: Remove the service policy from the interface and reapply it to the interface.

- CSCin83881

Symptoms: A VIP may crash on a Cisco 7500 series that is configured for dMLP.

Conditions: This symptom is observed when MLP member links flap while traffic is being processed.

Workaround: There is no workaround.

- CSCin88077

Symptoms: An active SP becomes stuck with an “sleep process” error when you enter the **test crash** command on the active RP.

Conditions: This symptom is observed on a Cisco Catalyst 6000 series that is configured with an ATA file system but is not platform-specific. The symptom occurs because of an error in the ATA file system.

Workaround: There is no workaround.

- CSCin88771

Symptoms: A router hangs while writing a crashinfo to a disk.

Conditions: This symptom is observed on a Cisco router that is configured with an ATA file system when the memory is corrupted. The router is unable to save MALLOC requests to a disk because the memory on the disk is corrupted, causing the router to hang.

Workaround: Configure the router in such a way that the crashinfo is written to bootflash memory. Ensure that there is sufficient space in the bootflash memory for the crashinfo.

- CSCin91163

Symptoms: Packets may be dropped as reassembly drops on a distributed (dMLP) ingress interface that has interleaving configured.

Conditions: This symptom is observed on a PA-MC-STM-1 port adapter when more than two DS0 members are part of an dMLP bundle that is configured for interleaving.

Workaround: There is no workaround.

- CSCin91381

Symptoms: A VIP that has a dMLFR configuration may crash when you enter the **microcode reload** global configuration command.

Conditions: This symptom is observed on a Cisco 7500 series when traffic flows through the VIP.

Workaround: There is no workaround.

- CSCin94305

Symptoms: When the standby RSP on a Cisco 7500 series boots while a Versatile Interface Processor (VIP) or other interface processor on the router reloads, the standby RSP reloads unexpectedly.

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0S, Release 12.2S, Release 12.2SB, Release 12.3T, Release 12.4, or Release 12.4T.

Workaround: There is no workaround.

- CSCin96583

Symptoms: After an OIR of a VIP on a Cisco 7500 series, MLP traffic causes a very heavy CPU load on the RP, in turn causing failures in the IPC configuration and memory allocation (malloc) failures.

Conditions: This symptom is observed on a Cisco 7500 series that is configured with a large number of distributed MLP bundles.

Workaround: There is no workaround.

- CSCin96590

Symptoms: A VIP crashes at the “free_wred_stats” function during an RPR+ switchover.

Conditions: This symptom is observed on a Cisco router that is configured with a VIP that has a configuration with about 12 MLP bundles with two T1 members when QoS is applied while traffic is flowing.

Workaround: There is no workaround.

- CSCin96692

Symptoms: On a Cisco 7500 series that is configured for dMLP, the txacc values of member interfaces may be wrongly credited to other member interfaces, causing RSP-3-RESTART messages, and finally causing traffic to stop.

Conditions: This symptom is observed when the member links flap continuously for some time while traffic is being processed.

Workaround: There is no workaround.

- CSCsa43329

Symptoms: A Cisco 12000 series may crash because of a bus error when you configure a loopback on one of the E3 interfaces on a 6-port E3 (6E3-SMB) or 12-port E3 (12E3-SMB) line card.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S.

Workaround: Do not configure a loopback on one of the E3 interfaces.

- CSCsa46484

Symptoms: A VIP or FlexWAN module in which a PA-POS-2OC3 port adaptor is installed may crash.

Conditions: This symptom is observed rarely and at random on a Cisco 7xxx series router or Cisco Catalyst 6000 series switch.

Workaround: There is no workaround.

- CSCsa53117

Symptoms: Multi-Layer Switching (MLS) CEF may stop functioning when an interface status changes. Ping and connectivity problems may also occur.

Conditions: This symptom is observed on a Cisco Catalyst switch and Cisco router when you shut down an interface or change VRF routes and as a result no other interfaces can be provisioned.

Temporary Workaround: Reload the Supervisor Engine or Route Processor.

- CSCsa57562

Symptoms: IPC messages may be generated on a 1-port channelized OC-12 (DS3) line card and the line card may be disabled and reload.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S or Release 12.0(28)SW1 when OC-3 subinterfaces are configured on the 1-port channelized OC-12 (DS3) line card, when these OC-3 subinterfaces are configured for Frame Relay, when the **rate-limit** command is enabled, and when L2TPv3 traffic is being processed.

Workaround: There is no workaround because the **rate-limit** command is not supported in a configuration in which L2TPv3 traffic is being processed.

- CSCsa58703

Symptoms: A number of AToM virtual circuits may not stay up after a configuration changes for a large number of AToM virtual circuits.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(31)S or Release 12.2SB.

Workaround: Flap the attachment circuit for each of the AToM virtual circuits.

- CSCsa59109

Symptoms: At random, subinterfaces lose the ability to ping a directly-connected peer.

Conditions: This symptom is observed on a Cisco 12000 series that is configured with two 3-port Gigabit Ethernet line cards.

Note that although regular and extended pings do not work, pings that use the record option do work.

Workaround: Reload microcode onto the affected line cards.

- CSCsa60026

Symptoms: Cells loss occurs on a single ATM link of PA-A3-8T1IMA or PA-A3-8E1IMA port adapter.

Conditions: This symptom is observed on a Cisco 7500 and 7200 series when one of the T1 or E1 member interfaces of an IMA group that is configured on a PA-A3-8T1IMA or PA-A3-8E1IMA port adapter is disconnected or when you enter the **shutdown** command on one of these T1 or E1 member interfaces. The symptom is not platform-specific and may also occur in other releases.

Workaround: There is no workaround.

- CSCsa61523

Symptoms: The following error message is generated on a Cisco 7200 series that has Multilink PPP (MLP) configured on serial interfaces of a PA-MC-STM-1 port adapter:

```
%SYS-2-BADSHARE: Bad refcount in datagram_done, ptr=3, count=0
```

Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.3(11)T3 only when MLP is configured on the serial interfaces. The symptom may also occur in other releases.

Workaround: Unconfigure MLP on the serial interfaces.

- CSCsa65360

Symptoms: During a high bit error rate (BER) condition, the controller of a PA-MC-8TE1+ port adapter remains up, which is not in compliance with the E1 and T1 standard.

Conditions: This symptom is observed when BER data is injected into an E1 or T1 port of a PA-MC-8T1E1+ port adapter. The state of the controller does not change to DOWN after 10 seconds of a continuous severely errored seconds (SES) condition.

Workaround: There is no workaround.

- CSCsa65819

Symptoms: The Label Information Base (LIB) may not be disabled.

Conditions: This symptom is observed on a Cisco router that is configured for MPLS VPN when an IPv4 BGP neighbor that is configured to exchange MPLS labels goes down.

Workaround: There is no workaround.

- CSCsa68616

Symptoms: An IPC failure occurs and an OC-12 line card that is configured for Frame Relay over MPLS resets.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(27)S1.

Workaround: There is no workaround.

Further Problem Description: The IPC failure and the line card reset occur after a depletion of the elements in the FrFab 608 byte queue for the line card. Consecutive outputs of the **show controllers slot-number frfab queue** command show a consistent and rapid leak of these buffers.

- CSCsa74044

Symptoms: An RP crashes during large interface configuration changes when interfaces and QoS policies are added or deleted.

Conditions: This symptom is observed on a Cisco 12000 series when the configuration changes involve ATM and serial interfaces.

Workaround: There is no workaround.

- CSCsa75285

Symptoms: A Cisco switch or router may crash when you install a 1-port multichannel STM-1, single mode port adapter (PA-MC-STM-1SMI) in a FlexWAN or VIP.

Conditions: This symptom is observed when you first power down the switch or router, install the PA-MC-STM-1SMI, and then boot up the switch or router.

Workaround: Install the PA-MC-STM-1SMI via an OIR procedure.

- CSCsa75375

Symptoms: You cannot configure the **speed** command on Ethernet interfaces.

Conditions: This symptom is observed on a Cisco 10720.

Workaround: There is no workaround.

- CSCsa77105

Symptoms: An LSP ping (or traceroute packet) is incorrectly sent from an unlabeled interface, preventing the LSP ping to detect LSP breakages when a one-hop label switched path is pinged.

Conditions: This symptom is observed on a Cisco router that is configured for MPLS OAM.

Workaround: There is no workaround.

- CSCsa77411

Symptoms: A crash that is related to MPLS TE bandwidth management may occur on a Cisco router which is configured for OSPF and MPLS Traffic Engineering.

Conditions: This symptom is observed on a Cisco router that integrates the fix for caveat CSCef16096 when the following conditions are present:

- The router is configured for OSPF and MPLS traffic engineering (TE).
- The interfaces, OSPF adjacencies, and TE tunnels are flapping.
- There are more than 300 OSPF interfaces (in any state, including administratively down) in the OSPF area that is configured for MPLS TE.

You can check the number of interfaces by entering the **show ip ospf** or **show ip ospf interface brief** command. Note that all interfaces that are covered by network statements are included in the command output, even those that are in the administratively down state.

A list of the affected releases can be found at

<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCef16096>. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

Workaround: There is no workaround.

- CSCsa80661

Symptoms: The data path on a 3-port Gigabit Ethernet Engine 2 (3GE-GBIC-SC) line card may be reset because of a corrupted packet that is found in the Tx SOP SRAM. This situation causes packet loss and the routing protocol sessions to flap.

Conditions: This symptom is observed on a Cisco 12000 series that runs a Cisco IOS software release that includes the fix for caveat CSCef06121. A list of the affected releases can be found at <http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCef06121>. Cisco IOS software releases that are listed in the “First Fixed-in Version” field at this location are affected.

Workaround: There is no workaround. The symptom causes a disruption of service, but service is restored.

Further Problem Description: When the symptom occurs, the following messages are generated in the log:

```
%RP-3-FABRIC_UNI: Unicast send timed out (1)
CORRUPT PACKET DUMP:
000005C000000000 0200000000000000 0000000101000000 00062AD9B40A0003
A09D008208004500 0000000000000000 0000000000000000 0000000000000000
0000000000000000 0000000000000000 0000000000000000 0000000000000000

%RPGE-6-AUTONEG_STATE: Interface GigabitEthernet1/0: Link OK -
autonegotiation complete
%RPGE-6-AUTONEG_STATE: Interface GigabitEthernet1/2: Link OK -
autonegotiation complete
%RPGE-6-AUTONEG_STATE: Interface GigabitEthernet1/1: Link OK -
autonegotiation complete
%LCGE-3-SOP_BAD_PACKET: Found corrupt pkts in tx-sop-sram. Data path was
reset.

%OSPF-5-ADJCHG: Process 1, Nbr 10.142.65.38 on GigabitEthernet1/0 from
LOADING to FULL, Loading Done
%OSPF-5-ADJCHG: Process 1, Nbr 10.142.65.44 on GigabitEthernet1/2 from
LOADING to FULL, Loading Done
```

- CSCsa82886

Symptoms: A router crashes when you enter the **tftp-server** command.

Conditions: This symptom is observed when the *filename* argument of the **tftp-server** command has a length of more than 67 characters.

Workaround: Ensure that the length of the *filename* argument does not exceed 67 characters.

- CSCsa83881

Symptoms: An interface of a PA-T3+ port adapter remains up during an Unavailable Seconds (UAS) condition that occurs because of a high C-bit or P-bit error rate.

Conditions: This symptom is observed on a Cisco 7200 series that is configured with a PA-T3+ port adapter.

Workaround: There is no workaround.

- CSCsa84587

Symptoms: A 6PE router crashes during an IPv6 ping to another PE router at the far side of the network.

Conditions: This symptom is observed when you enter the **no mpls ipv6 source-interface** command followed by **no interface type number** command in which the *type number* argument represents the IPv6 source interface that was configured in the **mpls ipv6 source-interface** command.

Workaround: When you want to disable the IPv6 source interface, first enter the **no interface type number** command in which the *type number* argument represents the IPv6 source interface that is configured in the **mpls ipv6 source-interface** command and then enter the **no mpls ipv6 source-interface** command.

- CSCsa86572

Symptoms: A large configuration in NVRAM on a primary or secondary RSP may become corrupted and the router may generate relevant warning messages during the execution of a **copy system:running-config nvram: startup-config** command.

When you erase NVRAM by entering the **erase nvram** command and then enter the **copy system:running-config nvram: startup-config** command, the router may crash.

Conditions: This symptom is observed on a Cisco 7500 series but is platform-independent.

Workaround: If the configuration file is significantly large, place a copy of the configuration file on a flash card or disk with ample space and enter the **boot config slot0:startup-config** command to force the startup configuration file to be read from the flash card.

When you enter the **copy system:running-config nvram: startup-config** command, the current running configuration is saved to the flash card or disk and the configuration is auto-synchronized to the corresponding flash card on the secondary RSP.

Caution: Do not remove the flash card while the **boot config slot0:startup-config** command is being executed.

- CSCsa87295

Symptoms: Traffic to a network core is dropped from a link-bundle interface of an Engine 3 line card.

Conditions: This symptom is observed when the network core is a Cisco 12000 series that runs Cisco IOS Release 12.0(26)S or a later release, that functions as a PE router, that is configured for MPLS VPN, and that has L3 loadbalancing enabled on an egress path through a link-bundle interface.

Workaround: There is no workaround.

Further Problem Description: The symptom occurs because there is incorrect FCR information in the Engine-3 hardware rewrites that point to the link-bundle interface.

- CSCsa88145

Symptoms: In some scalability cases with a large number of tunnels, SVIs, or VLANs, FIB tracebacks occur after an SSO switchover.

Conditions: This symptom is observed because traceback recording for the general event log and the interface event log is on by default.

Workaround: There is no workaround. Note, however, that there is no functional impact.

Further Problem Description: The fix for this caveat turns off traceback recording for the general event log and the interface event log.

- CSCsa88211

Symptoms: When you boot a Cisco 12000 series, some Layer 1 and CoS command are rejected with the following error messages:

```
Command "pos threshold sd-ber 9" not allowed on link-bundle member interface POS1/0
Command "tx-cos TEST" not allowed on link-bundle member interface POS1/0
```

Conditions: This symptom is observed on a Cisco 12000 series when a POS interface of an Engine 0 or Engine 2 line card has the **tx-cos** command enabled and is a member of a port channel or POS channel.

Workaround: There is no workaround.

- CSCsa88340

Symptoms: Unicast traffic that travels over an ATM subinterface between a PE router and a CE router stops.

Conditions: This symptom is observed on a Cisco 12000 series that functions as a PE router and that is configured with an ATM ISE line card when the following conditions are present:

- Remove the VRF that has only the ATM subinterface associated to it.
- Define a new VRF and remap the ATM subinterface to this new VRF.
- Enable RPF on the ATM subinterface.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the ATM subinterface or remove and re-add the ATM subinterface configuration.

- CSCsa91478

Symptoms: A Cisco 12000 series that is configured for L2TPV3 may continuously log the following CM_ERROR message, causing the syslog server to be flooded:

```
%SW_MGR-3-CM_ERROR: Connection Manager Error - unprovision segment failed
%SW_MGR-3-CM_ERROR: Connection Manager Error - unprovision segment failed
```

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(30)S1 when a Multilink Frame Relay (MFR) interface is shut down in the configuration of the **connect** command, causing proper provisioning to fail, unprovisioning to occur, and the error message to be generated.

Possible Workaround: Enter the **no shutdown** interface configuration command on the MFR interface.

- CSCsa93814

Symptoms: When you send a high rate of bidirectional unicast and multicast traffic, the PXF complex can crash and then recover on its own.

Conditions: This symptom is observed on a Cisco 10720 when a high rate of bidirectional unicast and multicast traffic is sent between GE ports across an SRP uplink.

Workaround: There is no workaround.

- CSCsa93883

Symptoms: No error condition is detected when a properly structured IPv4 packet has an invalid version value in the IP header. For example, IPv4 packets that have a version value other than 4 are forwarded without an error.

Conditions: This symptom is platform-independent and occurs under normal operating conditions.

Workaround: There is no workaround.

- CSCsa96275

Symptoms: When you send traffic with the full bandwidth of an IMA bundle, cell loss occurs. For example, cell loss occurs when you send traffic with more than 5 Mbps on an 8-link T1 IMA group or with 6.4 Mbps on an 8-link E1 IMA group.

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(30)S and that is configured for ATM L2TPV3, cell-packing, and multiple VP configurations. There is no cell loss with a single PVC without an L2TPv3 configuration.

Workaround: There is no workaround.

- CSCsa96941

Symptoms: When VBR ATM traffic is sent through a Cisco 12000 series 4-port ATM OC-3 ISE line card via an L2TPv3 IP tunnel to another 4-port ATM OC-3 ISE line card on another Cisco 12000 series, the VBR ATM traffic passes at lower rates than what is configured on the routers, and cell loss occurs.

Conditions: These symptoms are observed on a Cisco 12000 series that is connected back-to-back via an OC-192 POS link to another Cisco 12000 series.

Workaround: There is no workaround.

- CSCsa97090

Symptoms: A FIBNULLIDB error may occur on a Cisco platform that is configured for CEF.

Conditions: This symptom is observed under several conditions such as deleting a subinterface or performing an OIR of a new line card.

Workaround: There is no workaround.

- CSCsa97238

Symptoms: A 2.5G ISE SPA Interface Processor (SIP) in which a 4-port channelized T3 to DS0 Shared Port Adapter (SPA) is installed crashes when the controller is reconfigured and VRFs are present or have been present on the associated interfaces.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S.

Workaround: There is no workaround.

Further Problem Description: The SIP and SPA do not recover on their own; you must reload the router to recover the SIP and SPA.

- CSCsa99212

Symptoms: Traffic may continue to pass for a period of time on an AToM session even when the LDP session between two PE routers is disrupted.

Conditions: This symptom is observed on a Cisco router that functions as a PE router when it receives an LDP DOWN event.

Workaround: There is no workaround.

- CSCsa99983

Symptoms: New AToM or L2TPv3 sessions may not come up.

Conditions: This symptom is observed on a Cisco router that is configured for Multilink Frame Relay (MFR) over L2TPv3/AToM when there are services with incomplete MFR over L2TPv3/AToM configurations and when the router has run for a long period of time.

Workaround: There is no workaround.

- CSCsb00493

Symptoms: Packets do not switch through a core interface of a line card that has hardware acceleration enabled.

Conditions: This symptom is observed on a Cisco 12000 series when the line card that contains the core interface has also a VRF interface that is shut down.

Workaround: Disable hardware acceleration on the line card.

- CSCsb01188

Symptoms: An ATM subinterface on an ATM port adapter that is installed in a FlexWan module or VIP may transition to the down/down state.

Conditions: This symptom is observed on a Cisco Catalyst 6500 series, Cisco 7500 series, and Cisco 7500 series when you remove a QoS service policy from the ATM subinterface.

Workaround: There is no workaround.

- CSCsb02061

Symptoms: An “Output Hold Queue Wedge” condition may occur on PVCs that are defined on DS1 ports that are not configured for IMA.

Conditions: This symptom is observed on a Cisco 7200 series that runs the c7200-ik9s-mz image of Cisco IOS Release 12.3(13), that is configured with a PA-A3-8T1-IMA port adapter that is configured for DSL aggregation, and that terminates hundreds of UBR VCs on a DS1 interface. The “Output Hold Queue Wedge” condition occurs on idle subinterfaces or when multiple point-to-point subinterfaces are “spawned” from a single subinterface by entering a PVC range command such as the following:

```
interface ATM1/0.100 point-to-point
 ip unnumbered Loopback10
 atm route-bridged ip
 range pvc 6/100 6/599
```

There are four workarounds:

- Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the physical interface.
 - Enter the **no pvc-in-range** command followed by the **pvc-in-range** command on a wedged VC.
 - Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on an uplink interface.
 - Tear down and rebuild a PVC.
- CSCsb02753

Symptoms: Multicast traffic may be incorrectly dropped if it is filtered by an IPv6 ACL that matches on source and destination address.

Conditions: This symptom is observed when a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S and that performs IPv6 ACL filtering.

Workaround: Ensure that the **any** keyword is configured for the ACE instead of a source address, that is, enter the **permit protocol any multicast-ipv6-prefix/prefix-length sequence value** command.

- CSCsb02964

Symptoms: When a class map that contains an access control list (ACL) that is too large and complex to fit in memory is applied to an MQC policy map on a Cisco 10720, the router pauses indefinitely while compiling the ACL and generates a MALLOCFAIL error. The router should report an out-of-memory situation.

Conditions: This symptom is observed when the ACL contains 2000 lines and is complex.

Workaround: There is no workaround.

- CSCsb04721

Symptoms: When the Any Transport over MPLS (AToM) feature is enabled on a router, AToM virtual circuits to a peer may not be re-established after an interface flap or after being reconfigured, because the required targeted Label Distribution Protocol (LDP) session is not re-established.

Conditions: This symptom is observed when LDP is not configured on any interfaces via the **mpls ip** interface configuration command, which is typically the case when MPLS Traffic Engineering (TE) tunnels are used to transport AToM traffic between endpoints and when the **mpls ip** interface configuration command is not enabled on any TE tunnels.

The symptom occurs in Cisco IOS software releases that include the fix for caveat CSCec69982 when any form of one of the following commands is configured on the router and appears in the running configuration:

- **mpls ldp explicit-null**
- **mpls ldp advertise-labels**
- **mpls ldp session protection**
- **mpls ldp password fallback**
- **mpls ldp password option**
- **mpls ldp password required**

A list of the affected releases can be found at

<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCec69982>.

Workaround: Enter the **mpls ip** command on a TE tunnel interface or temporarily on a physical interface to force LDP to be re-established.

- CSCsb05218

Symptoms: An IPv6 ACL configuration may be lost or incorrect after an SSO switchover.

Conditions: This symptom is observed when a Cisco 12000 series performs IPv6 ACL filtering and when the ACL is modified.

Workaround: There is no workaround.

- CSCsb06383

Symptoms: When a high rate of multicast and unicast bi-directional traffic is sent into multiple access ports across an SRP uplink interface, the PXF engine may restart unexpectedly. Functionality is restored automatically.

Conditions: This symptom is observed on a Cisco 10720 that processes a high rate of multicast and unicast traffic.

Workaround: There is no workaround but the recovery is automatic.

- CSCsb09190

Symptoms: A router misses an entry in its label forwarding table, which is shown in the output of the **show tag-switching forwarding-table EXEC** command for the missing entry and in the output of the **show ip cef detail EXEC** command for the prefix.

Conditions: This symptom is observed on a Cisco router that is configured for Multiprotocol Label Switching (MPLS) and that learns its routes through iBGP from redundant route reflectors (RRs) when BGP labeling is not enabled.

Workaround: There is no workaround. However, when you enter the **clear ip route EXEC** command for the affected prefix, the prefix is reinstalled in the label forwarding table.

- CSCsb11124

The Cisco IOS Stack Group Bidding Protocol (SGBP) feature in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable denial of service condition. Devices that do not support or have not enabled the SGBP protocol are not affected by this vulnerability.

Cisco has made free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability.

Cisco has published a Security Advisory on this issue; it is available at <http://www.cisco.com/warp/public/707/cisco-sa-20060118-sgbp.shtml>

- CSCsb11568

Symptoms: On a 6PE router, an IPv6 ACL that is configured on an egress interface that faces a CE router does not filter any traffic.

Conditions: This symptom is observed on a Cisco 12000 series that is configured for 6PE when the egress interface is an interface of a line card that cannot process packets in its hardware, for example, an Engine 0 or Engine 2 line card.

Workaround: There is no workaround.

- CSCsb11574

Symptoms: After a Cisco 12000 series is rebooted, the interfaces that are associated with a 6-port channelized T3 (T1) line card may not come up.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S.

Workaround: Reload the line card to bring up the controllers and interfaces.

- CSCsb12969

Symptoms: All VIPs or FlexWAN modules reload unexpectedly on a platform that is configured for Modular QoS CLI (MQC).

Conditions: This symptom is observed on a Cisco 7500 series (with VIPs) and a Cisco 7600 series and Cisco Catalyst 6500 series (both with FlexWANs) when the following steps occur while the physical interface is in the UP state:

1. An input policy and output policy map are already attached to an ATM or Frame Relay PVC. When you attach the same policy map to the main interface, an error message is generated and the configuration is rejected.
2. You remove the policy map from the PVC and attach the same policy map to the main interface.
3. You remove the policy map from the main interface.

At this point, all VIPs or FlexWAN modules reload, even though no traffic is being processed during the above-mentioned steps.

Workaround: There is no workaround.

- CSCsb14213

Symptoms: When IPv4 multicast packets have a resultant IP checksum of "FFXX", the checksum becomes corrupt.

Conditions: This symptom is observed on a Cisco 10720 that runs Cisco IOS Release 12.0(31)S.

Workaround: There is no workaround.

- CSCsb17153

Symptoms: A serial interface that is configured for CRC-16 may revert to CRC-32 when a router reloads.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S when you configure a serial interface on a 4-port channelized T3 to DS0 SPA that is installed in a SIP-400 for CRC-16. When the configuration is saved and the router reloads, the interface comes up configured for CRC-32.

Workaround: There is no workaround.

- CSCsb17203

Symptoms: A Cisco 12000 series that is configured with dual PRPs, that has more than one 10G Engine 5 SPA Interface Processor (12000-SIP-600), and that has a 10-port Gigabit Ethernet (SPA-10X1GE) installed in each 12000-SIP-600 may not load one of the SPA modules after a cold boot.

Conditions: The symptom is observed only when the Cisco 12000 series is powered off and powered back on. The symptom does not occur on a Cisco 12000 series that is configured with a single PRP.

Workaround: Reload the router via a warm reload.

Further Problem Description: The symptom is related to a race condition that is only observed on the Cisco 12000 series. The symptom is more likely to occur when timing becomes an issue, for example, in a configuration with a large number of interfaces as described in the Symptoms above. However, the root cause of this race condition is platform-independent and relates to the interface IfIndex synchronization. This is the reason why the fix for this caveat is integrated in releases that do not support the Cisco 12000 series.

- CSCsb25404

Symptoms: The startup configuration in NVRAM is not loaded onto line cards when the router is manually reloaded.

Conditions: This symptom is observed on a Cisco 12000 series that functions as a multiservice edge (MSE) router when the ATM Cell Relay over MPLS feature is configured on 500 connections. The symptom may also occur on other platforms.

Workaround: After the router has been reloaded, cut and paste the initially rejected configuration onto the line cards.

- CSCsb27311

Symptoms: After you have send linerate traffic via an IMA interface for a while, a ping fails in a packed cell relay configuration via ATM over L2TPv3 pseudowires.

Conditions: This symptom is observed in a scalable packed cell relay configuration on an IMA interface of a PA-A3-8E1IMA or PA-A3-8T1IMA port adapter that is installed in a Cisco 7200 series or Cisco 7500 series.

Workaround: There is no workaround.

- CSCsb28139

Symptoms: An LDP/BGP adjacency is not formed, and a ping does not go through.

Conditions: This symptom is observed on a Cisco 12000 series that functions in a scaled VPN environment when an Engine 6 line card faces the core of the MPLS network.

Workaround: Enter the **clear ip route *** command.

- CSCsb29326

Symptoms: An snmpwalk for cmplsFrrFacObjects for the FRR-MIB fails to show entries for a tunnel headend.

Conditions: The symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(26)S6, Release 12.0(28)S3, or Release 12.0(31)S.

Workaround: There is no workaround.

- CSCsb33258

Symptoms: An RP crashes during BGP convergence when MVPNs are configured.

Conditions: This symptom is observed on a Cisco router after a duplicate BGP MDT extended community message is received that specifies a different Route Descriptor (RD) for an MDT that already exists for the specified MDT source and group address.

Workaround: There is no workaround.

- CSCsb34838

Symptoms: A line card or port adapter may generate SYS-6-STACKLOW error messages and reload because of a software forced crash. The crashinfo file shows that the crash is caused by the CEF Scanner process that is related to recursive calls:

```
%SYS-6-STACKLOW: Stack for process CEF Scanner running low, 0/6000
```

The output of the **show cef events** command for the line card or port adapter shows that a CPU hog condition occurs after the CEF Scanner process:

```
...
Process Scanner event loop enter
CPUHOG  -1ms XDRtyp 8=control len=11 Hex:0F0000079C00FA00
CPUHOG  2044ms XDRtyp 8=control len=13 Hex:08000000038E2A541A01
```

```
Flag      FIB switching running set to yes
+3d04h   CPUHOG   -4ms XDRtyp 69=TFIB_FRR_UNPROTECT_TRANSIT len=15
Hex:020001F400000000400000000
```

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(31)S.

Workaround: There is no workaround.

- CSCsb36081

Symptoms: An MFR link flaps when you remove and add a VLAN interface back on an SPA that is installed in an SPA Interface Processors (SIP).

Conditions: This symptom is observed on a Cisco 12000 series that is configured with a channelized T3 (to DS0) SPA that has both VLANs and an MFR configuration with Frame Relay subinterfaces. The SPA is installed in a SIP-400.

Workaround: There is no workaround.

- CSCsb39165

Symptoms: A Cisco router may report high CPU usage and memory depletion under a specific MPLS VPN configuration with static routes.

Conditions: This symptom is observed when equal cost static routes to a subnet point to a next hop address and there is a summary route that covers one of the next hops pointing to Null0.

If the directly connected route to the next hop is terminated because the interface goes down, the original route recurses to Null0 while the route recursing through the interface that is still up remains in the routing table. The end result is that the route now points to both Null0 and to a valid interface that is up, causing an MPLS recursion problem that results in high CPU usage and memory depletion.

The following is an example configuration:

```
ip route a.a.a.a b.b.b.b y.y.y.y
ip route a.a.a.a b.b.b.b z.z.z.z
ip route y.y.y.y mask Null0
```

If the directly connected route y.y.y.y is removed the a/b subnet recurses through the y.y.y.y/mask route to Null0.

Workaround: Use routes that point to both a next hop and an egress interface, as in the following example:

```
ip route a.a.a.a b.b.b.b interfaceY y.y.y.y
ip route a.a.a.a b.b.b.b interfaceZ z.z.z.z
```

Workaround: There is no workaround.

- CSCsb41367

Symptoms: When you enter the **redundancy force-switchover** command, an Engine 4 line card may crash.

Conditions: This symptom is observed on a Cisco 12000 series that runs the c12kprp-p-mz Cisco IOS software image and that has two RPs that function in SSO mode.

Workaround: There is no workaround.

- CSCsb42176

Symptoms: A Cisco 7200 series may pause indefinitely when a neighbor reloads.

Conditions: This symptom is observed on a Cisco 7200 series that is configured with a PA-POS-2OC3 port adapter.

Workaround: There is no workaround.

- CSCsb44220

Symptoms: During a high CPU load, the IPC ports on the RP are not opened, preventing CEF from communicating with a line card and causing a FIBDISABLE error message to be generated.

Conditions: This symptom is observed only when the router functions under high stress (that is, there is a high CPU Load on the RP and line cards) during bootup or when you perform an OIR of a line card, RP, or SP.

Workaround: There is no workaround.

Further Problem Description: Caveat CSCsb83521 resolves an issue that may occur if CSCsb44220 is integrated in an image. The issue concerns a scheduler error message.

- CSCsb46607

Symptoms: A standby route processor (RP) may crash in the “CEF LC IPC Background” process.

Conditions: This symptom is observed on a Cisco platform when an SSO switchover occurs.

Workaround: There is no workaround.

- CSCsb53420

Symptoms: Cell loss occurs when bursty VBR ATM traffic is sent through a Cisco 12000 series 4-port ATM OC-12 ISE line card via an L2TPv3 IP tunnel to another 4-port ATM OC-12 ISE line card on another Cisco 12000 series and when the VBR traffic is sent at rates lower than what is configured on the routers (that is, at about 50 percent of the OC-12 line rate).

Conditions: These symptoms are observed on a Cisco 12000 series that is connected back-to-back via an OC-192 or OC-48 POS link to another Cisco 12000 series.

Workaround: There is no workaround.

- CSCsb54190

Symptoms: When you shut down an SRP interface on which the egress L2 priority is set to high by entering the **no shutdown** interface configuration command, the PXF engine of a downstream router may crash.

Conditions: This symptom is observed on a Cisco 10720.

Workaround: Do not enter the **no shutdown** interface configuration command. Rather, force a ring wrap by entering the **srp ips forced-switch** command.

- CSCsb57467

Symptoms: When you shut down an interface that is configured uRPF in VRF verification mode, the VRF drop count increments.

Conditions: This symptom is observed only on a distributed Cisco platform when the **ip verify unicast vrf vrf-name permit/deny** command is enabled on the interface and when the uRPF VRF drop counter is non-zero when the interface is shut down.

Workaround: There is no workaround.

- CSCsb58311

Symptoms: An IMA port adapter may fail to receive data on a VC that is configured for cell packing with AAL0 encapsulation. The “ignored” counter in the output of the **show interface** command increments and the “rx_cell_throttle” count in the output of the **show controllers** command also increments.

Conditions: This symptom is observed when the Maximum Number of Cells Packed (MNCP) parameter is changed for a large number (around 100) of VCs.

Workaround: There is no workaround.

- CSCsb59294

Symptoms: The output is stuck on a Cisco 7200 series.

Conditions: This symptom is observed when a service policy attached to a T1 or E1 ingress interface on one of the following port adapters:

- PA-MC-2T1
- PA-MC-2E1/120
- PA-MC-4T1
- PA-MC-8T1
- PA-MC-8E1/120
- PA-MC-8TE1+

Workaround: Remove the service policy from the egress interface.

- CSCsb59555

Symptoms: An Engine 3 or Engine 4+ line card may be stuck in the “request reload” state and CEF may be disabled on the line card, although the CEF table is up, as is shown in the output of the **show cef linecard** command:

Slot	MsgSent	XDRSent	Window	LowQ	MedQ	HighQ	Flags
1	8558	719895	4966	0	0	0	up
2	8560	718293	4966	0	0	0	up
3	8609	722867	4965	0	0	0	up
4	8584	721311	4965	0	0	0	up
5	8597	724307	4965	0	0	0	up
9	8586	722060	4966	0	0	0	up
10	8579	720566	4966	0	0	0	up
11	8566	719086	4966	0	0	0	up
12	8606	725072	4966	0	0	0	up
13	8597	723572	4966	0	0	0	up
*7	1	3	24	0	0	0	disabled, rrp hold
0	4058	359354	4966	0	0	0	up

VRF Default, version 5032, 5024 routes

Slot	Version	CEF-XDR	I/Fs	State	Flags
1	5032	5016	67	Active	sync, table-up
2	5032	5016	5	Active	sync, table-up
3	5032	5016	20	Active	sync, table-up
4	5032	5016	5	Active	sync, table-up
5	5032	5016	5	Active	sync, table-up
9	5032	5016	4	Active	sync, table-up
10	5032	5016	4	Active	sync, table-up
11	5032	5016	20	Active	sync, table-up
12	5032	5016	4	Active	sync, table-up
13	5032	5016	8	Active	sync, table-up
*7	0	0	4	Active	table-disabled
0	0	0	5	Active	request reload, table-up

Conditions: This symptom is observed on a Cisco 12000 series after an RPR+ switchover has occurred. However, the symptom is platform-independent and may also occur on another platform that is configured for CEF when an RPR+ switchover has occurred.

Workaround: Enter the **clear cef linecard** command for the affected line card.

- CSCsb60714

Symptoms: The **mpls ldp router-id interface force** command is not accepted by the router.

Conditions: This symptom is observed on a Cisco 7200 series and Cisco 7500 series when the interface in the *interface* argument of the **mpls ldp router-id interface force** command is not yet configured. The symptom may also affect other platforms.

Workaround: First, configure the interface that you intend to use for the LDP router ID. Then, enter the **mpls ldp router-id interface force** command.

- CSCsb62041

Symptoms: A newly created channelized interface may show packet and byte counts before any traffic passes through the interface.

Conditions: This symptom is observed on a Cisco 12000 series. When a channelized interface is deleted, the interface index is released. This interface index may be re-allocated when a new channelized interface is created. The counters that are associated with the index need to be cleared when an interface is deleted so that they are properly initialized if the index is subsequently re-allocated to a new interface.

Workaround: There is no workaround. Although you can clear the interface counters via the CLI, doing so does not prevent the symptom from occurring because there is an internal counter that is used in the Tx byte and packet counts and that may cause errors in the calculations.

- CSCsb73181

Symptoms: A standby RP crashes and reloads when you apply an ATM QoS configuration.

Conditions: This symptom is observed on a Cisco 7304 that has two RPs and ATM line cards when an HA switchover occurs and when a QoS configuration is applied or changed.

Workaround: There is no workaround.

- CSCsb75433

Symptoms: Distributed Multilink PPP (dMLP) packets are not switched via dCEF.

Conditions: This symptom is observed on a Cisco router that is configured with multilink bundles.

Workaround: There is no workaround.

- CSCsb78898

Symptoms: A Cisco 10720 that functions as a transit router for MPLS applications such as MPLS VPN or AToM drops MPLS packets.

Conditions: This symptom is observed when the MPLS packets have multiple labels, when the egress interface on the Cisco 10720 has the **ip mtu bytes** command enabled, and when the MPLS packet size is greater than the value for the *bytes* argument.

Workaround: There is no workaround.

- CSCsb79325

Symptoms: An Engine 5 SPA enters the “FAILLC” state and resets when you shut down the main interface that is processing fragmented multicast traffic.

Conditions: This symptom is observed on a Cisco 12000 series when fragmented multicast traffic is forwarded across 500 VLANs (250 per port on two ports) and when the **no service auto-reset** command is enabled.

Workaround: There is no workaround.

- CSCsb83521

Symptoms: The following error message may be generated after an SSO switchover:

```
%SCHED-3-STUCKMTMR: Sleep with expired managed timer 55BE2914 time 0x1CD561
(00:00:00 ago).
-Process= "IPC LC Port Opener" ipl= 6 pid= 166
```

Conditions: This symptom is observed on a Cisco 12000 series that is configured for High Availability (HA).

Workaround: There is no workaround.

- CSCsb83876

Symptoms: The counters on a PA-MC-E3 port adapter may provide incorrect information. For some interfaces of the port adapter, the counters are always zero, and for others interfaces, the counters do increase but very slowly.

Conditions: This symptom is observed when you enter the **show interfaces type slot** command for a PA-MC-E3 port adapter.

Note that the symptom does not occur when you enter the **show interface type number stats** command or the **show interfaces type slot accounting** command. Also, when you enter the **show interfaces type slot** command for the VIP in which the PA-MC-E3 port adapter is installed, the counters provide correct information.

Workaround: Enter the **show interface type number stats** command to retrieve the correct information.

- CSCsb85338

Symptoms: When you perform an OIR of an alarm module or fan module, the inventory serial number (SN) may become lost after the new module is inserted, and the output of the **show inventory** command may not show the SN.

This situation prevents you from keeping track of the inventory and affects the operation of the Component Outage On-Line (COOL) feature.

Conditions: This symptom is observed on a Cisco 12000 series.

Workaround: There is no workaround.

- CSCsb89512

Symptoms: When an GE Engine 5 SPA forwards multicast traffic via multiple VLANs of one GE port, the content of IPv4 multicast packets becomes corrupted.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S.

Workaround: There is no workaround.

- CSCsb91678

Symptoms: A software-forced crash may occur on a Cisco 7206VXR because of a watchdog timeout.

Conditions: This symptom is observed on a Cisco 7206VXR that has a low-speed Mueslix-based serial port adapter such as a PA-4T+, PA-8T-V35, PA-8T-X21, or PA-8T-232 port adapter and that runs a Cisco IOS image that integrates the fix for caveat CSCec63468.

The symptom occurs only for low-speed port adapters such as the PA-4T+, PA-8T-V35, PA-8T-X21, and PA-8T-232 port adapters. The symptom may also affect port adapters in adjacent slots, and not only the port adapters in physically adjacent slots, but also the port adapters that are logically adjacent in the initialization path. This memory corruption occurs in the PCI/IO memory space.

A list of the affected releases can be found at

<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CScec63468>. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

Workaround: There is no workaround. Note that high-speed or unchannelized serial port adapters are not affected.

Further Problem Description: The following error messages and tracebacks are generated just before the crash occurs:

```
%SYS-2-BADSHARE: Bad refcount in datagram_done, ptr=3, count=0
-Traceback= 6074F79C 601BB3AC 601BC72C

%MUESLIX-1-HALT: Mx serial: Serial2/0 TPU halted: cause 0x3 status 0x0043404F shadow
0x630FB864

%ALIGN-3-SPURIOUS: Spurious memory access made at 0x6074F388 reading 0x1F
%ALIGN-3-TRACE: -Traceback= 6074F388 601BB3AC 601BC72C 00000000 00000000 00000000
00000000 00000000
%ALIGN-3-TRACE: -Traceback= 6074F7C0 601BB3AC 601BC72C 00000000 00000000 00000000
00000000 00000000

%SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = Per-Second Jobs.
-Traceback= 607E0078 607E44AC 607DACD0 601B0CD4 601B1A04 601ADEA8 603E2C2C 607CF128
6076E2EC
```

- CSCsb92374

Symptoms: When you enter the **no rd** command, the subsequent configuration or unconfiguration of the **rd** command for the VRF fails.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0S or Release 12.4 (no other releases are affected) when the **router bgp** and **address-family vpnv4** commands are not enabled and when the fix for caveat CSCeh12594 is integrated in the release. A list of the affected releases can be found at

<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCEh12594>. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

Workaround: Enter the **router bgp** command followed by the **address-family vpnv4** command.

Further Problem Description: The symptom occurs because a flag is set when you enter the **no rd** command for a VRF. Resetting the flag is essential to complete the process and occurs in a service routine that is registered only if the VPNv4 address family is configured for BGP. The fix for this caveat checks whether or not the VPNv4 address family is configured for BGP, and does not reset the flag if the VPNv4 address family is not configured for BGP.

- CSCsb94684

Symptoms: Packet drops may occur with random packet sizes on an SPA.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(30)S1 during a smartbits test with random packet sizes.

Workaround: There is no workaround. Note that the symptom does not occur in Cisco IOS Release 12.0(30)S.

- CSCsb95210

Symptoms: There is no traffic or traffic forwarded to an incorrect interface based upon the DSCP value of the IP packet.

Conditions: This symptom occurs when interfaces are deleted and added back with MQC.

Workaround: There is no workaround.
- CSCsb96092

Symptoms: When Virtual Router Redundancy Protocol (VRRP) is configured on a Cisco 12000 series and the FIB becomes disabled, VRRP becomes active in the groups for which it is configured and responds to ARP requests for the virtual address.

Conditions: This symptom is observed on a Cisco 12000 series when VRRP is configured and dCEF is disabled as a consequence of a memory allocation failure in the FIB.

Workaround: There is no workaround.
- CSCsb98254

Symptoms: A router may fail when you reload a Gigabit Ethernet (GE) line card or port adapter that has link-bundling enabled.

Conditions: This symptom is observed on a Cisco router when dot1q is configured on a GE interface of the line card or port adapter and when MPLS is enabled on an uplink.

Workaround: There is no workaround.
- CSCsb98654

Symptoms: The MQC may not take effect after you have applied a policy to an interface of a 4-port OC-48 POS Engine 4+ line card.

Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of an interim release for Cisco IOS Release 12.0(32)S.

Workaround: Reload the line card.
- CSCsc01577

Symptoms: Source Border Gateway Protocol Policy Accounting (BGPPA) counters do not increment.

Conditions: This symptom is observed on a Cisco 12000 series when you enter the **show cef interface type number policy-statistics** command.

Workaround: There is no workaround.
- CSCsc02825

Symptoms: In Cisco IOS software that is running the Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP), the router could reload while trying to access a bad virtual address.

Conditions: This symptom may be observed when LDP is being used. It will not be observed with TDP. It may happen when LDP receives a protocol message larger than 512 bytes right after receiving several Label Mapping messages smaller than 25 bytes. This problem is likely to be accompanied by the presence of one of the following error message:

Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0xD0D0D0D

The above error message may be preceded by one of the following four error messages:

```
%ALIGN-1-FATAL: Corrupted program counter
pc=0xD0D0D0D, ra=0x61164128, sp=0x64879B98
%TDP-3-BAD_PIE: peer x.x.x.x; unknown pie type 0x11E
%TDP-3-UNEXPECTED_PIE: peer x.x.x.x unexpected pie type 0x0
```



```
%TDP-3-PTCLREAD: peer x.xx.x0, read failure
```

This problem may be seen in releases that include the fix for CSCeg74562 but do not have the fix associated with this defect.

Workaround: There is no workaround.

- CSCsc05492

Symptoms: A GE Engine 2 line card that is configured for EoMPLS and the Carrier supporting Carrier feature with IPV4 BGP labels on two different dot1q subinterfaces may reset when you enter the **no hw-module slot slot-number shutdown** command on the line card.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S or a later release.

Workaround: There is no workaround.

- CSCsc05830

Symptoms: When a PE router has an output policy with the **mpls experimental number** command enabled on an egress interface that is configured for LDP, incoming IP packets that match the *number* argument are not selected and handled as default packets.

Conditions: This symptom is observed on a Cisco 10720 that functions as a PE router with a single output policy and no input policy.

Workaround: On the egress interface that is configured for LDP and that has the output policy, configure also an input policy.

- CSCsc06641

Symptoms: The following error messages and tracebacks are generated on the RP and line card of a Cisco 12000 series that processes IPv6 multicast traffic:

```
%SYS-2-MALLOCFAIL: Memory allocation of 3996 bytes failed from 0x50FFC814, alignment 0
Pool: Processor Free: 300276 Cause: Memory fragmentation
Alternate Pool: None Free: 0 Cause: No Alternate pool

-Process= "MFIB", ipl= 0, pid= 171
-Traceback= 501E0B58 50295620 5029A848 50FFC81C 50F78C20 50F78DE0 50FFDC30 50F78020
50F781F4 50F761D0 50F7588C 50F75BCC 50FFF194 50289CE4 50289CD0

-Process= "TAG Stats Background", ipl= 0, pid= 79
-Traceback= 40030E1C 400E3798 400E68D8 412A0B10 412A0F70

%SYS-2-CFORKMEM: Process creation of OBFL Coalesce failed (no memory).
-Process= "Logger", ipl= 0, pid= 25
-Traceback= 40030E1C 4011334C 401134F8 409F0868 409EFD78 409F15FC 409F175C 4002EFDC
4003170C
```

Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of an interim release for Cisco IOS Release 12.0(32)S.

Workaround: There is no workaround.

- CSCsc09436

Symptoms: An Engine 5 line card crashes when the Fabric MIB is polled.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S1 and only affects Engine 5 line cards.

Workaround: Create an SNMP View that excludes the Fabric MIB (CISCO-FABRIC-C12K-MIB).

- CSCsc11230

Symptoms: A Cisco 12000 series that is configured with a link bundle interface may generate a "FIB-3-LB_INTNOTEXIST" error message and traceback.

Conditions: This symptom is observed when any of the following conditions occur:

- A link-bundle member that contains subinterfaces is re-added to a port channel.
- A link-bundle member that contains subinterfaces is moved from one port channel to another.
- A normal Gigabit Ethernet interface that contains subinterfaces becomes a link-bundle member.

Workaround: There is no workaround.

Further Problem Description: The root cause of the symptom is any operation that involves the recreation of a subinterface re-creation with a link bundle.

- CSCsc14522

Symptoms: In a VPN topology, when you enter the **hw-module slot x qos interface queues 8** command on a 1-port channelized OC-12 (DS3) ISE line card, traffic does not go through MLP links.

Conditions: This symptom is observed on a Cisco 12000 series that runs an interim release for Cisco IOS Release 12.0(32)S.

Workaround: There is no workaround.

- CSCsc15449

Symptoms: An Engine 5 SPA continuously crashes when 2000 unique egress policies are applied to VLAN subinterfaces.

Conditions: This symptom is observed on a Cisco 12000 series and is related to a timing issue.

Workaround: There is no workaround.

- CSCsc16910

Symptoms: In an MVPN topology, an Engine 4+ POS line card that is located in the network core may punt packets with a size of 1477 bytes or more to its CPU.

Conditions: This symptom is observed on a Cisco 12000 series that runs an interim release for Cisco IOS Release 12.0(32)S.

Workaround: There is no workaround.

- CSCsc18661

Symptoms: When you send multicast traffic at or above 32 Kpps, the PXF buffers may deplete until they are exhausted.

Conditions: This symptom is observed on a Cisco 10720 when ACL logging is configured to deny multicast traffic at a rate of 32 Kpps and above.

Workaround: Do not use ACL logging for high-rate multicast streams.

- CSCsc20453

Symptoms: After an SSO switchover, interfaces of a channelized T1/E1 SPA go down and do not recover.

Conditions: This symptom is observed on a Cisco 12000 series that is configured with two PRP2 processors that function in SSO mode when you enter the **redundancy force-switchover** command.

Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the controller of the SPA to bring up the interfaces.

- CSCsc22726

Symptoms: A SIP-600 in which a 10-port Gigabit Ethernet SPA is installed resets because of an IPC timeout.

Conditions: This symptom is observed on a Cisco 12000 series when the SIP-600 is configured for VPLS and faces the core of the network. Note that the symptom does not occur with a 4-port Gigabit Ethernet ISE line card.

Workaround: There is no workaround.

- CSCsc25375

Symptoms: The fabric loader may crash.

Conditions: This symptom is observed on a Cisco 12000 series when you enter the **service download-fl** command.

Workaround: There is no workaround.

- CSCsc29637

Symptoms: An L2 overhead specification for shaping on a Gigabit Ethernet ISE line card is saved with the wrong syntax, and after you reload the router, this configuration is rejected.

Conditions: This symptom is observed on a Cisco 12000 series that runs an interim release for Cisco IOS Release 12.0(32)S.

Workaround: There is no workaround.

- CSCsc29914

Symptoms: You may not be able to ping across a serial T1 link that is configured on a channelized T3 SPA that is installed in a SIP-400.

Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of an interim release for Cisco IOS Release 12.0(32)S and that has the **ip routing external overload signalling** command enabled.

Workaround: Disable and then re-enable the **ip routing external overload signalling** command enabled.

- CSCsc30289

Symptoms: When the router at the opposite site is reloaded, a Dynamic Packet Transport (DPT) line card crashes because of a “Bus Error exception.”

Conditions: This symptom is observed on a Cisco 12000 series when the router at the opposite site is also configured with a DPT line card.

Workaround: There is no workaround.

- CSCsc32268

Symptoms: MPLS may fail when you remove Link Bundling from a Modular GbE Engine 4+ line card.

Conditions: This symptom is observed on a Cisco 12000 series that runs an interim release for Cisco IOS Release 12.0(32)S and that is configured for VPLS.

Workaround: Re-enable MPLS by entering the **mpls ip** global configuration command.

- CSCsc34114

Symptoms: When multicast QoS is configured on an egress interface of a POS or GE ISE line card and you reload the router, %EE48-3-ALPHAERR error messages are generated and traffic may not resume on the line card.

Conditions: This symptom is observed on a Cisco 12000 series that runs an interim release for Cisco IOS Release 12.0(32)S and that functions in an MVPN topology.

Workaround: There is no workaround.

- CSCsc34976

Symptoms: A PRP may reload because of a CPUvector 300 error.

Conditions: This symptom is observed on a Cisco 12816 that runs Cisco IOS Release 12.0(28)S1 and that is configured for QoS.

Workaround: There is no workaround.

- CSCsc36217

Symptoms: When you send IPv6 multicast traffic without hardware routes, the IPv6 multicast traffic is punted to the CPU of the line card without any hardware rate-limiting. This situation may cause the CPU of the line card to become overloaded.

Conditions: This symptom is observed on a Cisco 12000 series that is configured with Engine 3 and Engine 5 line cards.

Workaround: There is no workaround.

- CSCsc37404

Symptoms: An Engine 6 line card may reset with the following error messages:

```
%IPC-5-INVALID: NACK Source Port=0x403F0000
%MCC192-3-CPU_PIF: Error=0x4
%MCC192-3-CPUIF_ERR: Packet Exceeds Programmed Length.
%GSR-3-INTPROC: Process Traceback= 40D32E5C 406D8CE0
...
```

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S2.

Workaround: There is no workaround.

- CSCsc38678

Symptoms: When IS-IS IPv6 routes flap, a memory leak occurs on an ISE line card, eventually causing dCEF to be disabled when no more memory is available.

Conditions: This symptom is observed on a Cisco 12000 series that is configured with 180,000 BGP routes and 6000 IS-IS routes, 10 percent of which flaps each 30 seconds. The symptom occurs only when IS-IS flaps, not when BGP flaps. The symptom does not occur either when IPv6 routing is not configured.

Workaround: There is no workaround. If this is an option, remove IPv6 routing by entering the **no ipv6 unicast-routing** global configuration command. When the symptom has occurred and dCEF is disabled, you must reload the line card to restore its memory.

- CSCsc38929

Symptoms: Multicast Distributed Switching (MDS) may become disabled on one or more line cards, and the following error messages may be generated:

```
%SYS-2-WATCHDOG: Process aborted on watchdog timeout, process =
TCAM Mngr merge process.
-Traceback= 40030EFC 40112C80 401176A0 4010CB14 405FB2E0 405FC234 4069F47C 4069F6C4
406A12B4 406A2AA0 404E3950 404E57E8 404E59B0 404E5AD4 404F23A8 404FC7E4
--More--
%RP-4-RSTSLOT: Resetting the card in the slot: 1,Event: linecard error report
%QM-2-BAD_TLV: Error in internal messaging - bad tlv 0
%LINK-5-CHANGED: Interface POS1/0/0, changed state to administratively down
%LCINFO-3-CRASH: Line card in slot 1 crashed
```

The output of the **show ip mds stats linecard** command shows the MDS status. To reset the lMDS on the line card(s), enter the **clear ip mds linecard** command.

Conditions: This symptom is observed on a Cisco 12000 series that runs an interim release for Cisco IOS Release 12.0(32)S, that is configured with one or more Engine 5 line cards, and that has the following MQC outbound policy attached to an interface:

```
class-map match-all af11
  match ip dscp 10
class-map match-all cs1
  match ip dscp 8
  match ip precedence 1

policy-map check
  class af11
    bandwidth percent 10
    random-detect dscp-based
    random-detect dscp 10 10 packets 20 packets 1
  class cs1
    bandwidth percent 1
    random-detect dscp-based
    random-detect dscp 10 10 packets 15 packets 1
```

Workaround: There is no workaround.

- CSCsc42938

Symptoms: A router that is configured for Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) may crash when LDP is configured globally or on an interface.

Conditions: This symptom is observed when you enter the **show mpls ldp neighbor** command while LDP sessions are coming up or going down.

Workaround: There is no workaround.

- CSCsc44237

This caveat consists of two symptoms, two conditions, and two workarounds:

1. Symptom 1: A switch or router that is configured with a PA-A3 ATM port adapter may eventually run out of memory. The leak occurs when the FlexWAN or VIP that contains the PA-A3 port adapter is removed from the switch or router and not re-inserted.

The output of the **show processes memory** command shows that the “ATM PA Helper” process does not have sufficient memory. The output of the **show memory allocating-process totals** command shows that the “Iterator” process holds the memory.

Condition 1: This symptom is observed on a Cisco switch or router that runs a Cisco IOS software image that contains the fixes for caveats CSCeh04646 and CSCeb30831. A list of the affected releases can be found at

<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeh04646> and
<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeb30831>.

Cisco IOS software releases that are not listed in the “First Fixed-in Version” fields at these locations are not affected.

Workaround 1: Either do not remove the PA-A3 ATM port adapter from the FlexWAN or VIP or re-insert the PA-A3 ATM port adapter promptly. The memory leak stops immediately when you re-insert the PA-A3 ATM port adapter.

2. Symptom 2: A switch or router that has certain PIM configurations may eventually run out of memory.

The output of the **show processes memory** command shows that the “PIM process” does not have sufficient memory. The output of the **show memory allocating-process totals** command shows that the “Iterator” process holds the memory.

Condition 2: This symptom observed on a Cisco router that runs a Cisco IOS software image that contains the fix for caveat CSCef50104. A list of the affected releases can be found at <http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCef50104>.

Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

Workaround 2: When the **ip multicast-routing** command is configured, enable at least one interface for PIM. When the **ip multicast-routing vrf vrf-name** command is configured, enter the **ip vrf forwarding vrf-name** command on at least one interface that has PIM enabled.

- CSCsc46474

Symptoms: When you create a VRF, a router generates the following error message for a link bundle that does support MPLS VPN and that is configured on a 3-port Gigabit Ethernet (GE) Engine 2 line card:

```
%LC-6-PSA_UCODE_NO_SUPPORT: Current bundle does NOT support (MPLS VPN)
```

When you apply the VRF to an interface of the 3-port GE Engine 2 line card by entering the **ip vrf forwarding** command, the 3-port GE Engine 2 line card crashes.

Conditions: These symptoms are observed on a Cisco 12000 series that is configured with a port channel for link bundling.

Workaround: There is no workaround.

- CSCsc47733

Symptoms: A POS ISE line card crashes when you enter the **hw-module slot slot-number np mode feature** command.

Conditions: This symptom is observed on a Cisco 12000 series when you enter the above-mentioned command after you have configured and unconfigured a subinterface on the POS ISE line card.

Workaround: There is no workaround.

- CSCsc50401

Symptoms: A channelized T3 ISE line card in a Cisco 12000 series resets and when it comes back up, the MFR bundle link and the serial interfaces that belongs to the MFR bundle link remain in the down state.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S and that functions as a CE router in a MVPN topology when an interruption of service (such as an RP switchover) occurs on the neighboring router. This interruption of service causes the channelized T3 ISE line card to reset.

Workaround: To bring the interfaces up, enter the **microcode reload** command on the affected line card.

- CSCsc51691

Symptoms: After you have reloaded a Cisco 12000 series, a SIP-600 may fail.

Conditions: This symptom is observed on a Cisco 12000 series that runs an interim release for Cisco IOS Release 12.0(32)S and that is configured for VPLS when the SIP-600 processes traffic.

Workaround: There is no workaround.

- CSCsc52645

Symptoms: When Bit error rate testing (BERT) is configured on a timeslot or channel group, the entire T1 line goes down.

Conditions: This symptom is observed on a Cisco 7600 series and Cisco 12000 series that are configured with a channelized T3 to DS0 SPA.

Workaround: There is no workaround.
- CSCsc53661

Symptoms: After an RPR+ switchover has occurred, MFR interfaces that are configured on T1 and T3 SPAs that are installed in a SIP-601 may go down.

Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of Cisco IOS Release 12.0(32)S.

Workaround: Reload the subslots of the SIP-601 in which the SPAs are installed.
- CSCsc54514

Symptoms: All interfaces of the SPAs that are installed in a SIP-600 may be administratively down after an RPR+ switchover has occurred.

Conditions: This symptom is observed on a Cisco 12000 series that runs an interim release for Cisco IOS Release 12.0(32)S and that is configured with redundant RPs.

Workaround: There is no workaround.
- CSCsc54584

Symptoms: A standard ingress ACL for transit traffic does not function on an interface that is configured for MFR.

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.3(11)T8 and that has an MFR bundle that is configured on a PA-MC-8TE1 port adapter. The symptom may also occur in other releases.

Workaround: There is no workaround.
- CSCsc55477

Symptoms: When you regularly poll the ifHCInOctets MIB counter on a subinterface of a Modular GbE Engine 4 line card, the counter restarts at zero after the value 274651394019 (around 2³⁸) has been reached. The ifHCInOctets MIB counter is supposed to restart at zero after the value 2⁶⁴ has been reached.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S2.

Workaround: There is no workaround. Note that the symptom does not occur in Release 12.0(28)S5.
- CSCsc57753

Symptoms: An 1-port 10-Gigabit Ethernet Engine 4+ line card may crash when you perform an OIR by entering the **hw-module slot slot-number shutdown** command followed by the **no hw-module slot slot-number shutdown** command or when you enter the **microcode reload slot-number** command.

Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of Cisco IOS Release 12.0(32)S

Workaround: There is no workaround.

- CSCsc58973

Symptoms: When the **mpls ping** and **traceroute** commands are configured, the specified destination address does not take effect, nor is the 127.0.0.1 default address used when the destination address is not specified. Instead, the target FEC is used as the destination IP address in IP header of the outgoing packet.

When you specify a range of destinations for troubleshooting, the target IP address is always used. This situation prevents you from using the **mpls ping** and **traceroute** commands to troubleshoot an equal-cost multipath (ECMP) configuration.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0S.

Workaround: There is no workaround.

- CSCsc61616

Symptoms: A 1-port channelized OC-3/STM-1 Engine 5 SPA may crash when you delete an MLP bundle that has 12 links and that is configured on the SPA.

Conditions: This symptom is observed on a Cisco 12000 series when you perform an OIR of the SPA, enter the **hw-module reload** for the SPA, and then delete the MLP bundle from the SPA.

Workaround: There is no workaround.

- CSCsc63558

Symptoms: A 2-port OC-192 POS Engine 6 line card (the 2OC192/POS-SR-SC and the 2OC192/POS-IR-SC) may stop forwarding traffic after running properly for a while. When this situation occurs, the POS interface is in the UP/UP state, but a ping to the directly connected POS interfaces fails. No error messages are generated for the affected line card.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S2 or Release 12.0(28)S5, irrespective of whether or not an ACL is configured on the line card.

Workaround: There is no workaround. You must reset the line card to recover from the symptoms.

- CSCsc64384

Symptoms: Traffic does not flow on some ports (ports 6 through 9) of a 10-port Gigabit Ethernet Engine 5 SPA.

Conditions: This symptom is observed on a Cisco 12000 series that is configured with a SIP-601 that has 10-port Gigabit Ethernet Engine 5 SPAs in Bay 0 and Bay 1.

Workaround: There is no workaround.

- CSCsc64723

Symptoms: After an SSO switchover, traffic does not fully recover on a 3-port GE Engine 2 line card that is configured for EoMPLS.

Conditions: This symptom is observed on a Cisco 12000 series that runs the c12kprp-p-mz image of Cisco IOS Release 12.0(28)S5.

Workaround: Enter the **clear cef linecard slot-number** command to recover from the symptom and enable traffic to pass properly.

- CSCsc66887

Symptoms: All line cards on a Cisco 12000 series may reload when you configure a named ACL.

Conditions: This symptom is observed with the following configuration sequence:

1. You configure an IPv4 numbered (1-99) standard ACL.
2. You remove the IPv4 numbered standard ACL.

3. You configure a named IPv4 ACL.

Workaround: There is no workaround. Named ACLs are not supported on Cisco 12000 series line cards.

- CSCsc66938

Symptoms: Line cards reset continuously and the following error messages are generated:

```
%FIB-2-FIBDISABLE: Fatal error, slot 1: IPC Failure: timeout %RP-4-RSTSLLOT: Resetting the card in the slot: 1,Event: CEF failure
```

Conditions: This symptom is observed on a Cisco 12000 series when you boot the router with the c12kprp-p-mz image of an interim release for Cisco IOS Release 12.0(32)S.

Workaround: There is no workaround.

- CSCsc69537

Symptoms: A Cisco 12000 series may report incorrect ifIndex values in the NetFlow Data Export (NDE) packets that are sent from a Gigabit Ethernet (GE) ISE line card. Flows that arrive via VLAN subinterfaces may be reported as zero with the SNMP ifIndex or as the ifIndex of the physical GE interface.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(30)S3 or a later release after you have reloaded the GE line card.

Workaround: There is no workaround. When the symptom has occurred, re-apply the configuration of the subinterfaces.

- CSCsc70167

Symptoms: In an MVPN topology, a PE router that performs decapsulation may not forward multicast packets to a CE router.

Conditions: This symptom is observed on a Cisco 12000 series that runs an interim release for Cisco IOS Release 12.0(32)S.

Workaround: There is no workaround.

- CSCsc70802

Symptoms: Multicast traffic is dropped from an egress interface of an Engine 3 (ISE) and Engine 5 line card.

Conditions: This symptom is observed on a Cisco 12000 series.

Workaround for Engine 3 (ISE) line cards: Enter the **microcode reload slot-number** command.

Workaround for Engine 5 line cards: There is no workaround.

- CSCsc71547

Symptoms: A soft reboot may occur on a SIP-600.

Conditions: This symptom is observed on a Cisco 12000 series when you apply QoS policies on the SIP-600. The symptom occurs with any QoS policy (WRED, color, time stamping, and so on).

Workaround: There is no workaround.

- CSCsc72225

Symptoms: When you reload the core router in an MVPN topology, multicast traffic may not be switched via an ingress Engine 3, Engine 4+, or Engine 5 line card that is installed in the core router.

Conditions: This symptom is observed on a Cisco 12000 series runs Cisco IOS Release 12.0(32)S and that functions as a core router in an MVPN topology.

Workaround: Enter the **clear ip mds linecard** *linecard-slot-number* command, in which the *linecard-slot-number* argument represents the affected line card.

- CSCsc72960

Symptoms: A MAC address is not learned as expected after a microcode reload procedure is performed on a line card that is configured for VPLS.

Conditions: This symptom is observed on a Cisco 12000 series that functions as a core router.

Workaround: There is no workaround.

- CSCsc78355

Symptoms: After performing a manual switchover in RPR+ mode, the following error message may be generated continuously on an ISE line card and traffic is no longer forwarded:

```
%FIA-3-REQUESTERR: Request error was detected. Type = 1
```

Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of an interim release for Cisco IOS Release 12.0(32)S when the following conditions are present:

- The Cisco 12000 series functions as a PE router in an MVPN topology.
- The Cisco 12000 series performs decapsulation.
- The ISE line card is installed on the Cisco 12000 series and interconnects the router with a P router.

Workaround: Performing a microcode reload on the ISE line card.

- CSCsc78436

Symptoms: When you reload a channelized SPA, the following error message and traceback are generated:

```
%QM-2-TCAM_ERROR: TCAM pgm error(36): Invalid Parameters
```

Conditions: This symptom is observed on a Cisco 12000 series that is configured with an SPA that has MLP interfaces on which a service policy is attached.

Workaround: There is no workaround.

- CSCsc80380

Symptoms: When you configure a class policer in a child policy by entering the **police cir percent** command, the police rate calculation for the class may be incorrect.

Conditions: This symptom is observed on a Cisco 12000 series that has an hierarchical Modular QoS CLI (MQC) output service policy on the Ethernet interface of a shared port adapter (SPA).

Workaround: Configure the police rate explicitly in bits-per-second.

- CSCsc82431

Symptoms: The following traceback and error message may be generated when you reload an SPA or line card on which Multilink PPP (MLP) bundles are configured:

```
-Traceback= 406A2188 406A3670 406AA4E8 40339B28 4033C1D0 4033C374 40158D78 40159758
eelc_config_intf_tx_q(): EE_QM_QOS_INTERNAL_ERRORarg=3
```

```
%SPA_PLIM-3-HEARTBEAT: Subslot 0 has experienced an heartbeat failure Current
Sequence 14 received Sequence 8 Time since last keep 440ms
```

Conditions: This symptom is observed on a Cisco 12000 series that is configured for MLP and occurs irrelevant of whether or not the SPA or line card is processing traffic.

Workaround: There is no workaround.

- CSCsc85445

Symptoms: You cannot ping via some MFR interfaces and there is only unidirectional traffic through these MFR interfaces.

Conditions: This symptom is observed on a Cisco 12000 series that is configured with a 1-port channelized STM-1/OC-3 Engine 5 SPA and occurs after you have performed a microcode reload of the SIP in which the SPA is installed.

Workaround: There is no workaround. To recover from the symptoms, enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected MFR interfaces.

- CSCsc86645

Symptoms: The RP may crash when you change the MTU while the interfaces are coming up after you have reloaded an SPA or line card. This situation may cause the line protocol of all interfaces on the SPA or line card to remain down.

Conditions: This symptom is observed on a Cisco 12000 series that is configured for Multilink Frame Relay (MFR).

Workaround: There is no workaround.

- CSCsc88646

Symptoms: Traffic does not recover after an HA switchover, and the following ifIndex syslog message and traceback are generated:

```
%EERP-3-INVALID_INDEX: slot 0, port 1, vc -1 (type 68): index= 4096, maximum= 32
-Traceback= 1FB244 1FB34C 84C5CC 84D524 84D628 7FDD0C 7DC62C 329FBC 32ABFC 32AC88
2DAD9C 27E484 2E2C8C
```

Conditions: This symptom is observed on a Cisco 12000 series that is configured with the following features: IP, L3VPN, MLP, MR-APS, and mVPN.

Workaround: There is no workaround.

- CSCsc89318

Symptoms: MVPN traffic that traverses in the decapsulation direction is punted to the slow path on Engine 4+ line card that faces the core.

Conditions: This symptom is observed on a Cisco 12000 series that runs an interim release for Cisco IOS Release 12.0(32)S.

Workaround: There is no workaround.

- CSCsc99034

Symptoms: Traffic may not go through on VLAN-to-ATM and VLAN-to-Frame Relay links in AToM circuits that are configured for local switching.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(32)S.

Workaround: There is no workaround.

- CSCuk57124

Symptoms: An RP switchover may cause a CEF inconsistency on line cards.

Conditions: This symptom is observed on a Cisco router that has two PRPs that function in RPR+ redundancy mode.

Workaround: There is no workaround. If all line cards are affected, enter the **clear cef linecard** command to recover from the symptom. If a specific line card is affected, enter the **clear cef linecard slot-number** command to recover from the symptom. Enter these command from a console that is attached to the RP or RRP.

TCP/IP Host-Mode Services

- CSCsb51019

Symptoms: A TCP session does not time out but is stuck in the FINWAIT1 state and the following error message is generated:

```
%TCP-6-BADAUTH: No MD5 digest from x.x.x.x to y.y.y.y(179) (RST)
```

Conditions: This symptom is observed on a Cisco 12000 series that is configured for BGP and that is connected to a third-party vendor router after the BGP authentication password is changed on the Cisco 12000 series.

Workaround: There is no workaround.

- CSCsc39357

Symptoms: A Cisco router may drop a TCP connection to a remote router.

Conditions: This symptom is observed when an active TCP connection is established and when data is sent by the Cisco router to the remote router at a much faster rate than what the remote router can handle, causing the remote router to advertise a zero window. Subsequently, when the remote router reads the data, the window is re-opened and the new window is advertised. When this situation occurs, and when the Cisco router has saved data to TCP in order to be send to the remote router, the Cisco router may drop the TCP connection.

Workaround: Increase the window size on both ends to alleviate the symptom to a certain extent. On the Cisco router, enter the **ip tcp window-size bytes** command. When you use a Telnet connection, reduce the *screen-length* argument in the **terminal length screen-length** command to 20 or 30 lines.

Further Problem Description: BGP in Cisco IOS Release 12.0S and Release 12.4 is not affected because the retransmit timeout is disabled for BGP in these releases.

Wide-Area Networking

- CSCef54653

Symptoms: Some members of a multilink bundle remain inactive, while others are active.

Conditions: This symptom is observed when the interfaces are configured with the **ppp chap hostname** or **ppp multilink endpoint** command. Very high speed interfaces may come up and join the multilink bundle faster than the configuration can be processed, which causes them to use the host name of the router (instead of the configured user name or endpoint value) as the Endpoint Discriminator during Link Control Protocol (LCP) negotiations. This situation causes a mismatch between these links and those that come up after the configuration command is processed.

Workaround: Enter the **shutdown** interface configuration command followed by **no shutdown** interface configuration command on the active links to enable the links to renegotiate LCP with the correct Endpoint Discriminator value.

- CSCef71011

Symptoms: Pings fail when translational bridging and ATM DXI encapsulation are configured.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0S, Release 12.2S, or a release that is based on Release 12.2S.

Workaround: Do not configure ATM DXI encapsulation. Rather, configure HDLC, PPP, or Frame Relay encapsulation.

- CSCeh11994

Symptoms: A reply of an LNS to a LAC may be delayed.

Conditions: This symptom is observed on a Cisco router that is configured as an LNS that has several tunnels to different LACs.

Workaround: There is no workaround.

- CSCeh25440

Symptoms: InVARP packets on multiple MFR bundle interfaces may be dropped, causing traffic to fail after you have reloaded microcode onto a line card that processes a high load of traffic over many PVCs on MFR interfaces.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S when 42 MFR bundles are configured over 336 full T1s and when egress MQC is configured on the 42 MFR bundle interfaces. However, the symptom is not platform- and release-specific.

Workaround: There is no workaround.

- CSCeh34067

Symptoms: The Route Processor (RP) of a Cisco 7613 may crash when stress traffic is processed on all WAN links of FlexWANs in which channelized port adapters are installed and when interfaces of the channelized port adapters flap.

Conditions: This symptom is observed when the channelized port adapters are configured for MFR. The symptom may not be platform-specific.

Workaround: There is no workaround.

- CSCeh49616

Symptoms: Incoming MPLS packets with IETF Frame Relay encapsulation are process-switched.

Conditions: This symptom is observed only on a Cisco 7200 series.

Workaround: Do not configure IETF Frame Relay encapsulation. Rather, configure Cisco Frame Relay encapsulation.

- CSCeh49910

Symptoms: With automatic protection switching (APS) configuration on CHOC12 Internet Services Engine (ISE) cards, flapping the working link within a 2- to 3-second time interval may result in some of the T1 links staying down.

Conditions: This symptom has been observed with APS configuration on a CHOC12 ISE card.

Workaround: Enter a **shutdown** command and then a **no shutdown** command to clear the problem.

- CSCeh58376

Symptoms: A serial interface on a channelized port adapter may stop forwarding traffic through the router but traffic to and from the router over the interface may still go through. The Tx accumulator “value” counter in the output of the **show controllers cbus** Exec command does not exceed the value 2, as is shown in the following example:

```
Router#sh controllers cbus | include Serial5/1/0.1/2/6/2:0
Serial5/1/0.1/2/6/2:0, txq E8001B40, txacc E8000412 (value 2), txlimit 26
```

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0S when QoS is configured on at least one interface on the VIP in which the channelized port adapter is installed. The symptom occurs after the affected interface has flapped very frequently because of OSI layer 1 errors.

Workaround: Remove and reconfigure the controller of the affected interface.

- CSCei94893

Symptoms: AToM PVCs on an MFR interface that has keepalives disabled do not pass traffic after the router is rebooted.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0S.

Workaround: Enable LMI keepalives.

- CSCsa73905

Symptoms: The L2TP management daemon process may leak memory if the parsing of some L2TP control messages fails.

Conditions: This symptom is observed on a Cisco router that is configured for VPDN L2TP tunnels when PPPoE sessions were brought up and down after a period of time.

Workaround: There is no workaround.

- CSCsa87205

Symptoms: A router that is configured for PPP Multilink reloads because of a bus error.

Conditions: The exact conditions which caused the router to reload are unknown. It is believed to be triggered by a lack of free packet memory in the router.

Workarounds: There is no workaround.

- CSCsb61367

Symptoms: When you enter the **redundancy force-switchover** command on a router that is configured for PPP encapsulation, the IS-IS neighbor comes up in the INIT state.

Conditions: This symptom is observed on a Cisco router that is configured with two RPs that run in SSO redundancy mode.

Workaround: To bring up the IS-IS state in the IS-IS neighbor, enter the **isis protocol shutdown** interface configuration command followed by the **no isis protocol shutdown** interface configuration command on interface that provides the connection to the IS-IS neighbor.

Alternate Workaround: Configure HDLC encapsulation on the router.

- CSCsc33439

Symptoms: A virtual-access interface fails to come up after you have configured virtual templates.

Conditions: This symptom is observed on a Cisco router that is configured for MFR.

Workaround: There is no workaround.

- CSCsc52545

Symptoms: A VIP in which ATM port adapters are installed may crash.

Conditions: This symptom is observed on a Cisco 7500 series that is configured with two RPs that function in RPR+ mode.

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.0(31)S6

Cisco IOS Release 12.0(31)S6 is a rebuild of Cisco IOS Release 12.0(31)S. The caveats listed in this section are resolved in Cisco IOS Release 12.0(31)S6 but may be open in previous Cisco IOS releases. This section describes only severity 1, severity 2, and select severity 3 caveats.

Basic System Services

- CSCsb74471

Symptoms: IPC communication to an Engine 4 line card may be lost, the line card may reset, and an error message such as the following may be generated on the console of the RP:

```
%MDX-1-DAEMSGSNDFAILED: FAILED to send IPC message of TYPE MDX_DAE_PULL_REQ to slot 4 on the DAE, FAIL REASON = timeout
```

When the line card is in this state, the **execute-on** and **attach** commands do not function for the line card.

Conditions: This symptom is observed on a Cisco 12000 series that runs the c12kprp-p-mz image of Cisco IOS Release 12.0(27)S5 or Release 12.0(28)S5.

Workaround: Reset the line card.

IP Routing Protocols

- CSCea40884

Symptoms: A Cisco router may reload when you enter the **show ip route vrf vrf-name EXEC** command.

Conditions: This symptom is router- and release-independent.

Workaround: There is no workaround. However, if a single route must be displayed, enter the **show ip route vrf vrf-name prefix EXEC** command. Doing so may decrease the possibility that the router reloads. When you enter the **show ip route vrf vrf-name | in prefix EXEC** command, you may increase the possibility that the router reloads.

- CSCei83265

Symptoms: MVPN traffic is limited to about 9 Mpps and the CPU usage on the egress line card is 100 percent.

Conditions: This symptom is observed on a Cisco router that functions as a PE router when MVPN performs decapsulation in the slow path instead of the fast path.

Workaround: There is no workaround.

- CSCsc00378

Symptoms: Changes in an export map are not picked up by the BGP Scanner.

Conditions: This symptom is observed on a Cisco router that functions as a PE router when you apply an export map to a VRF and when the interface that connects the PE router to a CE router is configured for OSPF.

Workaround: Enter the **clear ip ospf process** command to enable the BGP Scanner to pick up the changes in the export map.

- CSCsc07467

Symptoms: An OSPF route is lost after an interface flaps.

Conditions: This symptom is observed rarely when all of the following conditions are present:

- There is a very brief (shorter than 500 ms) interface flap on a point-to-point interface such as a POS interface.
- The flap is not noticed by the neighbor, so the neighbors interface remains up.
- The OSPF adjacency goes down and comes back up very quickly (the total time is shorter than 500 ms).
- OSPF runs an SPF during this period and, based on the transient adjacency information, removes routes via this adjacency.
- The OSPF LSA generation is delayed because of LSA throttling. When the LSA throttle timer expires and the LSA is built, the LSA appears unchanged.

Workaround: Increase the carrier-delay time for the interface to about 1 second or longer.

Alternate Workaround: Use an LSA build time shorter than the time that it takes for an adjacency to come up completely.

- CSCsd03383

Symptoms: A route is not installed through an MPLS TE tunnel even though the **tunnel mpls traffic-eng autoroute announce** command is enabled.

Conditions: This symptom is observed on a Cisco router that also has the **mpls traffic-eng multicast-intact** command enabled.

Workaround: There is no workaround.

- CSCse65214

Symptoms: An RSVP Reservation message may be delayed.

Conditions: This symptom is observed on a Cisco router when an RSVP session is set up.

Workaround: There is no workaround.

Miscellaneous

- CSCef08173

Symptoms: A VIP in which a PA-2FE port adapter is installed may reload because of memory corruption that is caused by a hardware issue of the PA-2FE port adapter.

Conditions: This symptom is observed when the VIP and port adapter function under stress, when the VIP is unable to serve memory read/write requests from the port adapter, and when there are PCI retry timeouts.

Workaround: There is no workaround.

- CSCeg30179

Symptoms: Removing a policy that has shape and bandwidth in the same class (in that same order) may cause a router to crash.

Conditions: This symptom is observed when the router functions under a traffic load.

Workaround: There is no workaround.

- CSCeh29183

Symptoms: When you configure MPLS Traffic Engineering AutoTunnel Mesh Groups by entering the following commands, many FIB messages and tracebacks are generated:


```
mpls traffic-eng auto-tunnel mesh
mpls traffic-eng auto-tunnel mesh tunnel-num min 10000 max 20000
```

Depending on the configuration of the router and the topology, the symptom may also occur when you enter the following sequence of commands:

```
no mpls traffic-eng auto-tunnel mesh
mpls traffic-eng auto-tunnel mesh
no mpls traffic-eng auto-tunnel mesh
mpls traffic-eng auto-tunnel mesh
```

Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of a Cisco IOS interim release for Release 12.0(31)S.

Workaround: When you want to disable and then re-enable the **mpls traffic-eng auto-tunnel mesh** command, save the configuration and reload the router after you have disabled the command and before you re-enable the command, as in the following example:

```
no mpls traffic-eng auto-tunnel mesh
...
copy run start
reload
mpls traffic-eng auto-tunnel mesh
```

Similarly, when you want to change the range of unit numbers (that is, tunnel IDs) that is used by the **mpls traffic-eng auto-tunnel mesh** command, disable the command, change the range, save the configuration, reload the router, and then re-enable the command, as in the following example:

```
no mpls traffic-eng auto-tunnel mesh
mpls traffic-eng auto-tunnel mesh tunnel-num min 10000 max 20000
...
copy run start
reload
mpls traffic-eng auto-tunnel mesh
```

- CSCeh55186

Symptoms: MPLS TE LSPs may not come up and may remain stuck in the RSVP signaling proceeding state.

Conditions: This symptom is observed on a Cisco router when the MPLS TE LSPs are processed over inter-autonomous system broadcast links on which the **passive-interface** command is enabled.

Workaround: There is no workaround.

Further Problem Description: The **passive-interface** command contains the router ID of the remote Autonomous System Border Router (ASBR). A PATH message that leaves the passive interface of the Cisco router is sent to remote ASBR, causing an ARP request to be initiated for remote ASBR. However, there is no response to the ARP request (when there is no proxy configured for ARP), preventing the PATH message from reaching the remote ASBR.

- CSCej78720

Symptoms: A 4-port OC-48 POS Engine 4+ line card crashes repeatedly after you have entered the **microcode reload** command for all line cards in the router in succession.

Conditions: This symptom is observed on a Cisco 12000 series that runs an interim release for Cisco IOS Release 12.0(32)S and that functions as a PE router in an option 3 MPLS-(M)VPN Inter-AS environment when the affected line card has a core-facing interface.

Workaround: Perform a forced SSO switchover of the RP. Doing so stops the line card from crashing.

- CSCek04385

Symptoms: A 4-port OC-3 ATM ISE or 4-port OC-12 POS ISE line card on a PE router may crash when one of its egress interfaces that faces a P router is shut down while traffic is flowing.

Conditions: This symptom is observed on a Cisco 12000 series that functions as a PE router in an MPLS VPN environment, that is configured with a 4-port OC-3 ATM ISE or 4-port OC-12 POS ISE line card that faces the P router in the MPLS core, and that is configured with a 1-port OC-48 POS ISE line card that faces a CE router.

Workaround: There is no workaround.

- CSCek13657

Symptoms: The following error message may be generated when a router boots:

```
%SYS-2-NULLCHUNK: Memory requested from Null Chunk -Process= "Init", ipl= 3, pid= 3  
with an accompanying traceback.
```

Conditions: This symptom is platform- and release-independent and occurs when the router boots.

Workaround: There is no workaround. However, proper system operation is not affected.

- CSCek20952

Symptoms: The following error message may be generated when you configure a police statement in a policy map:

```
Maximum rate for the policer is 0, conform action is drop
```

Conditions: This symptom is observed on a Cisco router that functions in a L2VPN configuration with QoS features.

Workaround: There is no workaround.

- CSCek30891

Symptoms: Traffic loss may occur during reoptimization on a Cisco router that functions as a transit node for zero-bandwidth MPLS TE label switched paths (LSPs). The traffic loss stops when the TE tunnel headend switches traffic over to the new LSP.

Conditions: This symptom is observed on a Cisco router when reoptimization is triggered on the headend either periodically, manually, or as a result of a topology change.

Workaround: There is no workaround.

- CSCek32526

Symptoms: An Engine 6 line card may forward traffic to an incorrect destination port.

Conditions: This symptom is observed on a Cisco 12000 series that functions in a scaled configuration with 32,000 adjacencies, 770,000 single-path routes, and 99,000 4-path multi-path routes.

Workaround: There is no workaround.

- CSCek33205

Symptoms: OSPF adjacencies may be reset twice after an RPR+ switchover has occurred.

Conditions: This symptom is observed on a Cisco 12000 series when, after the OSPF adjacencies have been reset as expected because of the RPR+ switchover, the OSPF adjacencies are reset again because the core-facing interface reports an APS change state even without an APS configuration.

Workaround: There is no workaround.

- CSCek39754

Symptoms: Failures may occur on multiple DS3 interfaces of a 1-port CHOC-48 ISE line card. The line protocol on these interfaces may not come up, even not to an internal controller loop of the entire OC-48 circuit.

Conditions: These symptoms are observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S4 when dynamic provisioning is active.

Workaround: Reload the 1-port CHOC-48 ISE line card.

- CSCek39924

Symptoms: Duplicate processes are created for SONET alarm and Path Trace Buffer (PTB) handling on an Engine 4+ line card.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S or a later release.

Workaround: There is no workaround.

- CSCek40000

Symptoms: An interface may lose its QoS service policy.

Conditions: This symptom is observed on a Cisco 12000 series when you perform a basic operation such as shutting down the interface, reloading the line card, or performing an OIR of the line card.

Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, re-attach the service policy to the interface.

- CSCek42729

Symptoms: Multicast packets with certain ranges of packet sizes may be dropped. by an ISE line card.

Conditions: This symptom is observed on a Cisco 12000 series that functions as a PE router and that is configured with an ISE line card. The ISE line card has feature mode enabled and has an interface that connects to a CE router.

Workaround: Disable feature mode on the ISE line card.

- CSCek44541

Symptoms: PIM sessions fail to come up over a Data Multicast Distribution Tree (MDT).

Conditions: This symptom is observed on a Cisco router that functions as a PE router after you have entered the **clear ip bgp *** command.

Workaround: Enter the **clear ip mds linecard linecard-slot-number** command. For the *linecard-slot-number* argument, enter the core-facing slot.

- CSCek45970

Symptoms: In unidirectional mode, an Automatic Protection Switching (APS) switchover from a protect channel to a working channel may fail because the interface of the working channel remains in the up/down state.

Conditions: This symptom is observed on a Cisco 12416 that runs Cisco IOS Release 12.0(32)S3 and that has two redundant 1-port channelized OC-48 POS ISE line cards that are configured for APS.

Workaround: There is no workaround.

- CSCin96590

Symptoms: A VIP crashes at the “free_wred_stats” function during an RPR+ switchover.

Conditions: This symptom is observed on a Cisco router that is configured with a VIP that has a configuration with about 12 MLP bundles with two T1 members when QoS is applied while traffic is flowing.

Workaround: There is no workaround.

- CSCsc16910

Symptoms: In an MVPN topology, an Engine 4+ POS line card that is located in the network core may punt packets with a size of 1477 bytes or more to its CPU.

Conditions: This symptom is observed on a Cisco 12000 series that runs an interim release for Cisco IOS Release 12.0(32)S.

Workaround: There is no workaround.

- CSCsc34976

Symptoms: A PRP may reload because of a CPUvector 300 error.

Conditions: This symptom is observed on a Cisco 12816 that runs Cisco IOS Release 12.0(28)S1 and that is configured for QoS.

Workaround: There is no workaround.

- CSCsc79397

Symptoms: In an MVPN topology in which routers in the core are configured for PIM sparse mode with data MDT groups, an interruption in traffic in the core such as a reload of a P router may cause a PE router to stop sending traffic to the core.

Conditions: This symptom is observed when the traffic interruption causes the traffic to fall back to the default MDT and PIM sparse mode to enter the registering state. When the traffic resumes before the multicast route for the data MDT group times out, the traffic is initially forwarded over the default MDT and then switched to the data MDT, but no PIM registration control packets are sent.

Workaround: Enter the **clear ip mds linecard linecard-slot-number** in which the *linecard-slot-number* argument is the ingress line card on the affected PE router.

Further Problem Description: We recommend the use of Source Specific Multicast (SSM) for data MDTs. Using SSM, you can avoid the symptoms entirely.

- CSCsd13490

Symptoms: An Engine 2 line card may crash when it receives multicast traffic that is not punted to the CPU of the line card but switched by the PSA memory of the line card.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(27)S or a later release when the Engine 2 line card is configured with the wrong PSA memory and when you enable multicast hardware acceleration by entering the **hw-module slot slot-number ip multicast hw-accelerate** command.

Workaround: Disable multicast hardware acceleration on Engine 2 line card.

- CSCsd16581

Symptoms: An Engine 3 or Engine 5 line card may crash while processing packets for Output Sampled NetFlow.

Conditions: This symptom is observed on Cisco 12000 series when Output Sampled NetFlow is enabled on the Engine 3 or Engine 5 line card and when packets are sampled that are not aligned to a 2-byte boundary.

Workaround: Disable Output Sampled NetFlow.

- CSCsd21134

Symptoms: A Cisco 12000 series line card may crash while processing packets that are not aligned to a 4-byte boundary.

Conditions: This symptom is observed when the packet is processed in the CPU of the line card.

Workaround: There is no workaround.

- CSCsd25480

Symptoms: A 1-port 10GE SPA may send packets with random source MAC addresses.

Conditions: The symptom is observed intermittently on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S2 and that is configured with 1-port 10GE SPAs that are installed in a SIP-600.

Workaround: There is no workaround.

- CSCsd75069

Symptoms: The IPC link between a SIP and its SPAs may fail, an “RX IPC FIFO FULL” error message and heartbeat failure error messages may be generated, and all interfaces on the SPAs that are installed in the SIP may go down.

Conditions: This symptom is observed when a large number of channel interfaces are defined on the SPAs and when traffic with small packet sizes is passing at a high rate (near line rate) through the SIP.

Workaround: There is no workaround. To recover from the symptoms, reload the affected SPAs or reload the SIP.

- CSCsd83355

Symptoms: Multicast packets may be lost intermittently on a Cisco 12000 series. On average, one packet may be lost per minute per multicast stream.

Conditions: This symptom is observed on Engine 4+ and Engine 5 line cards.

Workaround: Reroute the traffic.

- CSCsd88973

Symptoms: A traffic interruption in an MVPN core such as a reload of a P router may prevent a connected PE router that functions as a PIM neighbor from re-establishing a connection with other PE routers.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S2.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface of the P router that has been reloaded and that connects to the PIM neighbor.

- CSCse06191

Symptoms: When you configure FRoMPLS on a 4-port CHOC-12 ISE line card, the line card may reload continuously.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0S or Release 12.0(32)SY.

Workaround: There is no workaround.

- CSCse08081

Symptoms: A Cisco 7200 series that has a service policy on a channelized interface may reload unexpectedly.

Conditions: This symptom is observed on a Cisco 7200VXR that runs Cisco IOS Release 12.0(31)S4 or Release 12.0(32)S and that is configured with an NPE-G1 and a PA-MC-8TE1+ port adapter. The symptom may also affect other releases of Release 12.0S. The symptom occurs only under the following conditions:

- A CBWFQ service policy is applied to a channelized interface of the PA-MC-8TE1+ port adapter.

- The router is booted with the service policy applied to the interface (that is, the service policy is defined in the startup configuration).
- Traffic is congesting the channelized interface.

Workaround: After the router comes up, remove and re-apply the service policy to the channelized interfaces.

Alternate Workaround: Do not boot the router with the service policy applied to the interface but apply the service policy after the router has booted.

Further Problem Description: See also caveat CSCse08092.

- CSCse08092

Symptoms: A header buffer leak may occur on a Cisco 7200 series that has a service policy on a channelized interface. You can verify the leak in the output of the **show buffers | i Head** command by looking at the total number of header buffers that are in use:

```
Header pools: Header buffers, 0 bytes (total 30650, permanent 256):
```

```
Header pools: Header buffers, 0 bytes (total 33086, permanent 256):
```

Conditions: This symptom is observed on a Cisco 7200VXR that runs Cisco IOS Release 12.0(31)S4 or Release 12.0(32)S and that is configured with an NPE-G1 and a PA-MC-8TE1+ port adapter. The symptom may also affect other releases of Release 12.0S. The symptom occurs only under the following conditions:

- A CBWFQ service policy is applied to a channelized interface of the PA-MC-8TE1+ port adapter.
- The router is booted without the service policy applied to the interface (that is, the service policy is not defined in the startup configuration).
- Traffic is congesting the channelized interface.

Workaround: Remove the service policy from the channelized interface.

Further Problem Description: See also caveat CSCse08081.

- CSCse09498

Symptoms: When you enter the **no shutdown** interface configuration command on an auto-template interface during deployment, some tunnels may be in the up/down state, and the tunnel mode may be GRE instead of the configured tunnel mode of MPLS.

Conditions: This symptom is observed on a Cisco router with about 70 primary MPLS TE tunnels. The symptom occurs when you first enter the **no interface auto-template** command, then you enter the **tunnel mode mpls traffic-eng** command, and finally you paste the template back.

Workaround: Reload the router.

Alternate Workaround: Create an automesh in the following sequence:

```
conf t
access-list 60 permit 10.0.7.3
access-list 60 permit 10.0.1.5
access-list 60 permit 10.0.2.6
access-list 60 permit 10.0.3.7
access-list 60 permit 10.0.5.1
access-list 60 permit 10.0.6.2
access-list 60 permit 10.0.8.12

interface Auto-Template1
ip unnumbered Loopback0
no ip directed-broadcast
tunnel destination access-list 60
tunnel mode mpls traffic-eng
```

.....

```
access-list 60 permit 10.0.7.3
access-list 60 permit 10.0.1.5
access-list 60 permit 10.0.2.6
access-list 60 permit 10.0.3.7
access-list 60 permit 10.0.5.1
access-list 60 permit 10.0.6.2
access-list 60 permit 10.0.8.12
```

- CSCse33664

Symptoms: A multichannel T1 or E1 port adapter may become deactivated when you enter the **invert data** or **crc 16** interface configuration command.

Conditions: This symptom is observed on a Cisco 7500 series that is configured with an RSP4 that contains an R5000 microprocessor.

Workaround: There is no workaround.

- CSCse35036

Symptoms: An interface of a 2-port OC-192 POS Engine 6 line card may stop sampling NetFlow.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco OS Release 12.0(28)S6.

Workaround: Remove NetFlow from the affected interface and then re-apply NetFlow to the interface.

Resolved Caveats—Cisco IOS Release 12.0(31)S5

Cisco IOS Release 12.0(31)S5 is a rebuild of Cisco IOS Release 12.0(31)S. The caveats listed in this section are resolved in Cisco IOS Release 12.0(31)S5 but may be open in previous Cisco IOS releases. This section describes only severity 1, severity 2, and select severity 3 caveats.

Basic System Services

- CSCeg11566

Symptoms: Intensive SNMP polling may cause the I/O memory of a router to be depleted.

Conditions: This symptom is observed in rare situations.

Workaround: Reduce the SNMP polling interval, frequency, or rate.

- CSCei77083

Symptoms: A spurious memory access may be generated on an RSP when a VIP that is in a disabled or wedged condition is recovered because of a Cbus Complex or microcode reload.

Conditions: This symptom is observed on a Cisco 7500 series that has a VIP that is in a disabled or wedged condition after the router has booted.

Workaround: There is no workaround.

Interfaces and Bridging

- CSCei68284

Symptoms: POS interfaces may remain in the up/down state after the router has been reloaded.

Conditions: This symptom is observed on a Cisco Catalyst 6500 series, Cisco 7500 series, and Cisco 7600 series.

Workaround: Reload the FlexWAN or VIP in which the POS port adapter is installed.

- CSCsc30369

Symptoms: A cBus Complex Restart may occur on a Cisco 7500 series when you leave the interface configuration mode after you have changed the encapsulation on a serial interface from HDLC to another encapsulation type such as PPP or Frame Relay.

The maximum datagram for an interface a of low-speed serial port adapter with HDLC encapsulation and an MTU of 1500 is 1528 because the overhead that is added to the MTU is 28. The maximum datagram for an interface a of high-speed serial port adapter with HDLC encapsulation and an MTU of 1500 is 1530 because the overhead that is added to the MTU is 30.

When the encapsulation type is changed, the maximum datagram size may change, which causes an internal MTU change. This situation may cause some packets to be dropped as giants.

Conditions: This symptom is observed after the first change to the type of encapsulation from the default of HDLC to another encapsulation type when you leave the interface configuration mode. Subsequent changes to the type of encapsulation do not cause the cBus Complex Restart.

Workaround for the cBus Complex Restart: There is no workaround for the cBus Complex Restart. An MTU change on a Cisco 7500 series results in a cBus Complex Restart, which usually means a router outage of 15 to 30 seconds or a minute and a half, depending on the Cisco IOS software image that the router is running.

Workaround for the packet drops: Reconfigure the MTU to prevent packet from being dropped as giants.

Further Problem Description: The fix for this caveat ensures the maximum datagram for an interface a of low-speed serial port adapter with HDLC encapsulation and an MTU of 1500 is 1608 to allow for an overhead to the MTU of 108. The maximum datagram for an interface a of high-speed serial port adapter with HDLC encapsulation and an MTU of 1500 is then 1610 to allow for an overhead to the MTU of 110.

- CSCsd49253

Symptoms: A Cisco 7200 series may reload unexpectedly when an Automatic Protection Switching (APS) switchover occurs on Packet over SONET (POS) interfaces that are configured for redundancy.

Conditions: This symptom is observed on a Cisco 7200 series.

Workaround: There is no workaround.

IP Routing Protocols

- CSCsb50606

Symptoms: Memory utilization in the “Dead” process grows gradually until the memory is exhausted. The output of the **show memory dead** command shows that many “TCP CBs” re allocated. Analysis shows that these are TCP descriptors for non-existing active BGP connections.

Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.3(13), that has an NPE-G1, and that functions as a PE router with many BGP neighbors. However, the symptom is not platform-specific, nor release-specific.

Workaround: Reload the router. If this is not an option, there is no workaround.

- CSCsc73598

Symptoms: The IGP metric is not updated to an eBGP peer when there is an IGP- metric change. The BGP peer is not advertising this change after its default timer of 10 minutes.

Conditions: This symptom occurs when a link goes down and the IGP metric to reach the BGP nexthop has changed. When used in a route-map, the **set metric-type internal** value should propagate any MED changes in updates to the BGP peers.

Workaround: Use **clear ip bgp neighbor-address [soft [in | out]]** on the respective router to get the correct metric changes and BGP best path.

- CSCsc74229

Symptoms: A router may delete the VPNv4 prefixes from the BGP table, even though the counters in the output of the **show ip bgp** command may indicate that the VPNv4 prefixes are present in the BGP table. This situation may cause loss of VPN connectivity.

Conditions: This symptom is observed on a Cisco router that is configured for MPLS VPN and that functions as a PE router.

Workaround: There is no workaround. When the symptom occurs, enter the **clear ip bgp *** command to restore proper operation of the router.

Miscellaneous

- CSCef35269

Symptoms: A Cisco 7500 series that has a multichannel E1 port adapter that is configured with PPP multilink groups on several E1 channels may drop packets:

- When dCEF is enabled, packets that are larger than 1492 bytes are dropped. Note that this particular symptom is addressed and fixed via CSCin73658.
- When the router has dCEF disabled, packets that are larger than 1500 bytes are dropped.

Conditions The symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(28)S.

Workaround: Configure only one interface as the member of the PPP multilink group. Note that the symptom does not occur in Release 12.0(26)S3, 12.0(27)S2, and 12.1(19)E1.

- CSCef82084

Symptoms: Spurious memory accesses occur on a Cisco 7200 series and ALIGN-3-SPURIOUS error messages are generated.

Conditions: This symptom is observed when there is traffic through the serial interface.

Workaround: There is no workaround.

- CSCeh31441

Symptoms: A linecard reloads when traffic is sent through an ATM PVC with the QoS policy enabled.

Conditions: The symptom occurs only with the following configuration.

```
policy-map foo
  class class-default
    shape average <cir>

interface atm1/0/0.
  pvc <vpi>/<vci>
```

```
service-policy output foo
```

Workaround: Add a dummy class to the policy-map with a bandwidth or shape feature as shown in the following example:

```
policy-map foo
  class dummy
    bandwidth <kbps>
  class class-default
    shape average <cir>
```

- CSCej16004

Symptoms: An MTU change on a multilink bundle interface takes no effect for SPA interfaces. This situation may cause the traffic to be dropped.

Conditions: This symptom is observed on a Cisco 12000 series when you change the MTU on a multilink bundle interface and when you change the traffic generation accordingly.

Workaround: There is no workaround.

- CSCek28323

Symptoms: An interface of an Engine 3 ingress line card that functions in feature mode may become stuck, and all traffic may be dropped.

Conditions: This symptom is observed on a Cisco 12000 series that is configured with an Engine 3 ingress line card that has the **hw-module slot slot-number np mode feature** command enabled and that is configured with an egress line card that has a link bundle interface.

Workaround: Disable the **hw-module slot slot-number np mode feature** command on the Engine 3 ingress line card.

- CSCek30152

Symptoms: When a T3/E3 Serial SPA is configured in Kentrox mode with a small bandwidth between 22 kbps and 250 kbps, either in T3 or E3 mode, the firmware miscalculates the bandwidth allocation and allows up to 24M of traffic to pass through.

Conditions: This symptom is observed on a Cisco 7304 and a Cisco 12000 series.

Workaround: Do not configure such a small bandwidth when the T3/E3 Serial SPA is configured in Kentrox mode. The minimal bandwidth on a T3/E3 Serial SPA that is configured in Kentrox mode is either 1500 kbps in T3 mode or 1000 kbps in E3 mode.

- CSCek30377

Symptoms: A SIP may generate an error message or crash when you first perform an OIR of an SPA-10X1GE that is installed in the SIP and you then enter the **show tech-support** command.

Conditions: This symptom is observed on a Cisco 12000 series.

Workaround: Suggested workarounds:

- Issue each command separately that makes up the **show tech** set of commands. Doing so will avoid the command **show hw-module subslot all brief** due to which the crash happens.
- Shut down SIP-600 and then OIR the spa. This will result in the other spa in the SIP-600 getting reloaded as well.

Further Problem Description: The symptom does not occur when a 1-port OC192/STM64 POS/RPR SPA is installed in the SIP.

- CSCek31439

Symptoms: If the sender and receiver for a multicast group are on the same line card on a PE router, the v flag may be set, causing traffic to be punted to the RP.

Conditions: This symptom is observed on a Cisco 12000 series when a hash collision occurs. The symptom may not be platform-specific.

Workaround: There is no workaround.
- CSCek31489

Symptoms: MQC ingress policing may not filter multicast traffic.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(32)S when the MQC policy map is configured on an OC-12 subinterface of a 1-port channelized OC-48 ISE line card in the ingress direction.

Workaround: There is no workaround.
- CSCek37693

Symptoms: The **speed** command cannot be configured on FE interfaces.

Conditions: This symptom has been seen on a Cisco 7500 series router with a PA- 2FE-TX in a VIP4-80. The FE port is connected to a switch port. If the switch port is set for 10MB and the FE interface is unable to be manually configured with the **speed** command, the FE interface will be in an up/down state.

Workaround: Use the **speed auto** command on the switch port that connects to the FE interface on the router. By using this workaround, you will not be able to throttle the bandwidth to 10MB as desired. The interface will be up/up, and will pass traffic at 100MB.
- CSCek38260

Symptoms: Routers may crash with MPLS VPN configuration and shutting down PE-CE link.

Conditions: The symptoms may occur when the router acts as a PE on the MPLS VPN topology and when one or more PE-CE links are shut down.

Workaround: There are no workaround.
- CSCin96524

Symptoms: Control plane traffic may be dropped from a multilink interface.

Conditions: This symptom is observed only when the multilink interface is oversubscribed and does not occur under normal traffic conditions.

Workaround: Reduce the traffic rate.

Alternate Workaround: Apply some type of queueing mechanism on the interface.
- CSCsa46484

Symptoms: A VIP or FlexWAN module in which a PA-POS-2OC3 port adaptor is installed may crash.

Conditions: This symptom is observed rarely and at random on a Cisco 7xxx series router or Cisco Catalyst 6000 series switch.

Workaround: There is no workaround.
- CSCsa63173

Symptoms: CEF may not be updated with a new path label that is received from the BGP peer.

If a router configured for BGP IPv4+labels multipath receives a BGP update that only changes the MPLS label for a non-bestpath multipath, the router fails to update the forwarding plane. This results in dropping or mis-branding the traffic.

Conditions: In a IPv4+labels multipath setup, if a label is changed for the non-bestpath multipath and that is the only change in the new update received from the neighbor, the new label will not be programmed in forwarding, hence there will be label inconsistency between the BGP and the forwarding tables.

Workaround: There is no workaround.

- CSCsb52900

Symptoms: An inconsistency may occur in the outlabel information that is used by BGP and MPLS forwarding.

Conditions: This symptom is observed when there are two route reflectors (RRs) that advertise the same route and when one of the routes is the best path. The symptom occurs when the following conditions are present:

- The PE router that is the source restarts, causing the prefix to be readvertised with a new label.
- The RR that forms the non-best path delays the withdrawal and readvertisement of the prefix, for example, because the RR has a heavy load.

This situation causes BGP to function with the new label but MPLS forwarding to function with the old label.

Workaround: Enter the **clear ip route** *network* command for the affected prefix.

- CSCsc16318

Symptoms: When you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on all serial interfaces of an MLP bundle, a ping fails because OSPF is stuck in the INIT state.

Conditions: This symptom is observed even while the MLP bundle comes up after you have entered the **no shutdown** interface configuration command.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the main interface of the MLP bundle.

- CSCsc40236

Symptoms: Incorrect outgoing labels are installed for BGP-IPv4 Multipath prefixes.

Conditions: This symptom has been observed anytime that a label changes from a BGP-IPv4 Multipath peer.

Workaround: Clearing the BGP neighbor should allow the correct labels to be installed.

- CSCsc50401

Symptoms: A channelized T3 ISE line card in a Cisco 12000 series resets and when it comes back up, the MFR bundle link and the serial interfaces that belongs to the MFR bundle link remain in the down state.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S and that functions as a CE router in a MVPN topology when an interruption of service (such as an RP switchover) occurs on the neighboring router. This interruption of service causes the channelized T3 ISE line card to reset.

Workaround: To bring the interfaces up, enter the **microcode reload** command on the affected line card.

- CSCsc94359

Symptoms: The BGP table and CEF forwarding table may have mismatched labels for prefixes that are learnt from a remote PE router.

Conditions: This symptom is observed on a Cisco router that functions as a PE router when an eBGP session flap or route flap occurs on the remote PE router. A new label for the prefix is learnt from the remote PE router, but forwarding may not be updated properly.

Workaround: There is no workaround. When the symptom has occurred, and to correct the situation, enter the **clear ip route vrf vrf-name network** command on the PE router that has mismatched labels.

- CSCsd11646

Symptoms: On a router that runs Multiprotocol Label Switching (MPLS), the "%SYS-3-OVERRUN:" and "%SYS-6-BLKINFO" error messages may be generated and a software-forced crash may occur on the router.

Conditions: This symptom is observed when you enter the **show mpls ldp discovery** command under the following condition:

- There are multiple LDP adjacencies configured through one interface.
- The adjacencies between peers through this interface have not been fully established for some peers.
- The unestablished LDP adjacencies are coming while you enter the **show mpls ldp discovery** command.

Workaround: Do not enter the **show mpls ldp discovery** command while multiple LDP adjacencies are coming up. Rather, enter the **show mpls ldp neighbor [detail]** command while multiple LDP adjacencies are coming up.

- CSCsd12941

Symptoms: The CPU usage may remain at 99 percent for a long time when NMS polls the ipRouteTable via the SNMP protocol.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(28)S or Release 12.0(31)S when there is a large number of routes in the routing table. The symptom may also occur in other releases.

Workaround: Exclude the ipRouteTable from the SNMP view.

- CSCsd20210

Symptoms: The PXF engine of a Cisco 10720 may crash.

Conditions: The symptom is observed when you modify an existing access control list (ACL) that is attached to an interface.

Workaround: Do not modify an ACL that is attached to an interface. If you cannot remove the ACL from the interface, create a new ACL and apply it to the interface.

- CSCsd23189

Symptoms: The **ip helper-address** command does not function on a 4-port Gigabit Ethernet ISE line card (4GE-SFP-LC).

Conditions: This symptom is observed on a Cisco 12000 series when the Gigabit Ethernet interface is configured for VRF forwarding.

Workaround: There is no workaround.

- CSCsd34463

Symptoms: An Engine 4, Engine 4 plus, or Engine 6 line card may punt MPLS packets to the RP, causing the CPU usage of the RP to be high.

Conditions: This symptom is observed on a Cisco 12000 series that receives a large number of small MPLS packets that have their TTL set to 1.

Workaround: There is no workaround.

- CSCsd35405

Symptoms: A line card that is configured with a multilink bundle may reset when the connected serial T1 interface on the remote router is shut down while traffic is flowing.

Conditions: This symptom is observed on a Cisco 12000 series when the traffic that enters the multilink bundle exits over an L2TPv3 tunnel and when multilink fragmentation is applied at the remote end.

Workaround: Disable multilink fragmentation at the remote end. If this is not an option, there is no workaround.

- CSCsd36528

Symptoms: In an MVPN topology, an Engine 5-based SIP (that is, a SIP-401, SIP-501, SIP-600, or SIP-601) in which one or more SPAs are installed may reset when you forward multicast traffic with packets that are larger than the MTU of the interface and therefore require fragmentation.

Conditions: This symptom is observed on a Cisco 12000 series, that functions as a PE router, and that is located in the network core when a SPA that is installed in the SIP interconnects the PE router with a P router.

Workaround: There is no workaround.

- CSCsd37840

Symptoms: When a Cisco 7500 series that runs in SSO mode reloads (for example, because of a “c7500 CCB PLAYBACK” error), the active RP comes up properly but the standby RP crashes. When the router reloads while running in RPR+ mode, the standby RP does not crash but an “%HA-3-SYNC_ERROR: CCB Playback error” message is generated.

Conditions: This symptom is observed on a Cisco 7500 series that is configured for SSO or RPR+.

Workaround: There is no workaround. The symptom does not occur when you disable SSO or RPR+.

- CSCsd47404

Symptoms: When configuring output ACL in an interface of an E4+ EPA-GE/FE-BBRD card, the following error message is shown. However, the output of **show tcam-mgr gen7 appl acl-out block-info** shows that there are 964 free entries in TCAM.

```
SLOT 9:Feb 23 00:07:54: %FM-3-TCAM_FAIL: Write label: 0, direction:
egress to TCAM error:
failed to program all entries (partly programmed). Performance will be
seriously degraded for traffic hitting ACL rules beyond hardware capability.
-Process= "Feature Manager", ipl= 0, pid= 46 -Traceback= 40030CBC
404EB828 404E419C 404E4784 SLOT 9:Feb 23 00:08:01: %FM-3-TCAM_FAIL:
Write label: 0,
direction: egress to TCAM error:
failed to program all entries (partly programmed). Performance will be
seriously degraded for traffic hitting ACL rules beyond hardware capability.
-Process= "Feature Manager", ipl= 0, pid= 46 -Traceback= 40030CBC
```

Conditions: This symptom has been observed in an E4+ LC card when the line card does not find enough free sequential entries in TCAM at its current location because of ACL expansion and needs to relocate ACL to a different location within the TCAM.

Workaround: Perform a workaround similar to the example which follows:

An example configuration of **access-list 102** and **103** applied on GigabitEthernet interface at 9/0/1.

1. Remove all of the ACL applied to that line card interfaces globally.

```
config terminal
no access-list number [number = 102, 103]
```

2. Remove all of the ACL configuration from the line card interfaces.

```
config terminal
interface GigabitEthernet 9/0/1
no ip access-group number out [number = 102, 103]
```

3. On line card confirm that the ACLs have been removed.

```
show access-lists gen7-fm label
```

4. Recreate the ACL globally, which are the ACL deleted in Step 1.

5. Re-apply the ACL configuration to the LC interfaces, the one's deleted in Step 2.

6. On the line card, confirm that the ACLs have been recreated properly.

```
show access-lists gen7-fm label
```

- CSCsd49374

Symptoms: When you reload a channelized T3 SPA that is installed in a PE router, all interfaces on a directly-connected channelized T3 SPA that is installed in a CE router remain in the down state, and the following error message is generated:

```
%SPA_CHOC_DSX-3-SPA_CMD_SEND_ERR: Failed to send ipc_send_rpc_blocked command to SPA
```

Conditions: This symptom is observed in a VPN topology on a Cisco 12000 series that runs Cisco IOS Release 12.0(32)S1, that functions as a PE router, and that is connected to another Cisco 12000 series that functions as a CE router. The channelized T3 SPA in the PE router is installed in a SIP-601; the channelized T3 SPA in the CE router is installed in a SIP-400.

Workaround: Reload the channelized T3 SPA in the CE router.

- CSCsd57040

Symptoms: When the controller of multichannel T3 port adaptor SPA-4XCT3 goes down for a short duration and an alarm occurs, the port adaptor does not report the type of alarm.

Conditions: This symptom has been observed on Cisco 7600 series and Cisco 12000 series routers that are configured with a SPA-4XCT3. The port adaptor should provide a history table of recent alarm conditions along with a corresponding time stamp to allow for proper troubleshooting.

Workaround: There is no workaround.

- CSCsd71119

Symptoms: ATM PVCs configured with OAM on the FlexWAN module/PA-A3-OC3 might go down. This occurs because OAM cells are not being received correctly on the ATM PVCs. The ATM interface remains up/up, but the subinterfaces with PVCs configured go down/down.

Subinterfaces with PVCs without OAM configured remain up/up, but the traffic does not pass.

Conditions: This symptom has been observed on a Catalyst 6500 switch running Cisco IOS Release 12.2SXF.

Workaround: A reset of the interface and/or a reset or reload of the FlexWAN module might resolve the issue.

- CSCsd82249

Symptoms: In MPLS VPN topology, where E3 4xOC12 ATM line card is a Core-facing line card, after performing a reload on any of Egress line cards, the ATM line card may reload.

Conditions: This symptom has been observed on a E3 4xOC12 ATM line card configured with MPLS Aware Netflow, on a Cisco 12000 series that runs Cisco IOS Release 12.0(32)S2 or 12.0(32.1)S4.

Workaround: There is no workaround.

Wide-Area Networking

- CSCeh34067

Symptoms: The Route Processor (RP) of a Cisco 7613 may crash when stress traffic is processed on all WAN links of FlexWANs in which channelized port adapters are installed and when interfaces of the channelized port adapters flap.

Conditions: This symptom is observed when the channelized port adapters are configured for MFR. The symptom may not be platform-specific.

Workaround: There is no workaround.

- CSCeh49616

Symptoms: Incoming MPLS packets with IETF Frame Relay encapsulation are process-switched.

Conditions: This symptom is observed only on a Cisco 7200 series.

Workaround: Do not configure IETF Frame Relay encapsulation. Rather, configure Cisco Frame Relay encapsulation.

- CSCeh58376

Symptoms: A serial interface on a channelized port adapter may stop forwarding traffic through the router but traffic to and from the router over the interface may still go through. The Tx accumulator “value” counter in the output of the **show controllers cbus** Exec command does not exceed the value 2, as is shown in the following example:

```
Router#sh controllers cbus | include Serial5/1/0.1/2/6/2:0 Serial5/1/0.1/2/6/2:0, txq E8001B40, txacc E8000412 (value 2), txlimit 26
```

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0S when QoS is configured on at least one interface on the VIP in which the channelized port adapter is installed. The symptom occurs after the affected interface has flapped very frequently because of OSI layer 1 errors.

Workaround: Remove and reconfigure the controller of the affected interface.

- CSCsd21476

Symptoms: A router crashes when you attempt to delete a Frame Relay-to-Ethernet connection.

Conditions: This symptom is observed when you first remove the Frame Relay interface via an OIR and then you attempt to delete the Frame Relay-to-Ethernet connection.

Workaround: Re-insert the Frame Relay interface before attempt to delete the Frame Relay-to-Ethernet connection.

Resolved Caveats—Cisco IOS Release 12.0(31)S4

Cisco IOS Release 12.0(31)S4 is a rebuild of Cisco IOS Release 12.0(31)S. The caveats listed in this section are resolved in Cisco IOS Release 12.0(31)S4 but may be open in previous Cisco IOS releases. This section describes only severity 1, severity 2, and select severity 3 caveats.

Basic System Services

- CSCed44414

Symptoms: When the slave RSP crashes, a QAERROR is observed in the master console, resulting in a cbus complex. The cbus complex will reload all the VIPs in the router.

Conditions: This symptom happens when the slave crashes in a period when there is a large number of packets going towards the RSP. A large number of packets go to the RSP when CEF switching is configured or when routing protocol updates are numerous.

Workaround: There is no workaround.

- CSCee41892

Symptoms: A VIP4-80 card may fail to load the Cisco IOS software image. When this situation occurs, the following error messages are generated:

```
%DBUS-3-SW_NOTRDY: DBUS software not ready after HARD_RESET, elapsed 13056, status 0x0
%DBUS-3-WCSLDERR: Slot 2, error loading WCS, status 0x4 cmd/data 0xDEAD pos 97
%DBUS-3-WCSLDERR: Slot 2, error loading WCS, status 0x4 cmd/data 0xDEAD pos 99
%UCODE-3-LDFAIL: Unable to download ucode from system image in slot 2, trying rom
ucode
%RSP-3-NOSTART: No microcode for VIP4-80 RM7000 card, slot 2
```

Conditions: This symptom is observed on a Cisco 7500 series when you enter the **microcode reload** command.

Workaround: There is no workaround.

Further Problem Description: The symptom may also occur because of improperly installed line cards. If this situation occurs, re-install the line cards.

- CSCej08355

Symptoms: The active Supervisor Engine or Route processor (RP) may reload when the standby Supervisor Engine or RP is inserted.

Conditions: This symptom is observed on a Cisco switch or router when the following conditions are present:

- The SSO redundancy mode is configured.
- The **snmp mib notification-log default** command is enabled.

Workaround: Do not configure SSO as the redundancy mode. Rather, configure RPR+ as the redundancy mode.

Alternate Workaround: Disable the SNMP MIB notification log by entering the **no snmp mib notification-log default** command.

- CSCin86930

Symptoms: Incoming ATM traffic is dropped from interfaces of an ATM port adapter because the usage of the CPU increases to 100 percent on the VIP.

Conditions: This symptom is observed on a Cisco 7500 series that is configured with 1000 ATM AAL5 over MPLS (AAL5oMPLS) VCs and that processes 1000 pps (512 kbps) of traffic.

Workaround: There is no workaround.

- CSCsa98777

Symptoms: An MSFC may reload when the standby Supervisor Engine 720 is inserted. Similarly, the active Route Processor (RP) may reload when the standby RP is inserted.

Conditions: These symptoms are observed on a Cisco Catalyst switch or router when SNMP and SSO are configured, and when the following configuration is present on the platform:

```
snmp mib notification-log default
snmp mib notification-log globalageout 600
snmp mib notification-log globalsize 1500
```

Workaround: Do not configure SSO. Rather, configure RPR+.

Alternate Workaround: Remove the SNMP MIB notification-log configuration by entering the **no snmp mib notification-log default** command.

- CSCsb14026

Symptoms: A standby RSP reloads continuously.

Conditions: This symptom is observed on a Cisco 7500 series that is configured for SSO and that has the **snmp mib notification-log default** command enabled.

Workaround: Disable the **snmp mib notification-log default** command.

- CSCsc14034

Symptoms: The active RP crashes during the boot process.

Conditions: This symptom is observed on a Cisco router that is configured for SSO and that has the **snmp mib notification-log default** command enabled.

Workaround: Disable the **snmp mib notification-log default** command.

Interfaces and Bridging

- CSCsa54176

Symptoms: Spurious memory accesses are generated on a VIP when the RSP sends traffic such as routing updates or non-dCEF switched traffic through VLAN subinterfaces.

Conditions: This symptom is observed on a Cisco 7500 series that is configured with an RSP when the following conditions are present:

- The router dCEF enabled.
- 802.1Q VLAN subinterfaces are configured on Fast Ethernet or Gigabit Ethernet interfaces.
- The VLAN subinterfaces have an output service policy configured.

Workaround: There is no workaround.

- CSCsc17534

Symptoms: Unicast packets are not CEF-switched on a VIP but are fast-switched on the RP.

Conditions: This symptom is observed on a Cisco router that has a VIP only when the ingress interface is an ISL subinterface.

Workaround: There is no workaround.

- CSCsc69537

Symptoms: A Cisco 12000 series may report incorrect ifIndex values in the NetFlow Data Export (NDE) packets that are sent from a Gigabit Ethernet (GE) ISE line card. Flows that arrive via VLAN subinterfaces may be reported as zero with the SNMP ifIndex or as the ifIndex of the physical GE interface.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(30)S3 or a later release after you have reloaded the GE line card.

Workaround: There is no workaround. When the symptom has occurred, re-apply the configuration of the subinterfaces.

IP Routing Protocols

- CSCef60452

Symptoms: A router may stop receiving multicast traffic.

Conditions: This symptom is observed rarely during convergence when a router receives a Join message on an RPF interface and when a downstream router converges faster than the first router that receives the Join message.

In this situation, the router does not populate the RPF interface into the OIL (that is, the OIL remains null) because the old SP-tree has already been pruned by the downstream router. When the RPF interface of the router changes to the new path later, it does not trigger a Join message toward the multicast source until the router receives a next periodic Join message from the downstream router and populates the OIL. As a result, multicast traffic stops temporarily but no longer than the periodic Join message interval.

Workaround: There is no workaround.

- CSCsb79749

Symptoms: The output of the **show memory summary** command may contain garbled characters in the “What” column.

Conditions: This symptom is observed when you configure OSPF with at least one network, and then unconfigure it.

Workaround: There is no workaround.

- CSCsc59089

Symptoms: BGP does not advertise all routes to a peer that sends a route-refresh request.

Conditions: This symptom is observed under the following conditions:

- The router is in the process of converging all of its peers and has updates ready in the output queue for the peer.
- The peer sends a route-refresh request to the router. This may occur when the **clear ip bgp * soft in** command is entered on the peer or when a VRF is added to the peer.
- The router processes the route-refresh request from the peer while the router still has updates in the output queue for the peer.

In this situation, all of prefixes that are advertised by the unsent updates in the output queue for the peer are lost.

Workaround: There is no workaround. When the symptom has occurred, enter the **clear ip bgp * soft out** command on the router to force the router to send all updates to its peers.

ISO CLNS

- CSCsc63871

Symptoms: When IS-IS and CLNS are configured, a router may enter a state in which only one adjacency is shown in the output of the **show clns interface** command, even though the **show clns neighbors** command may correctly display all the neighbors that are connected to the interface.

When this situation occurs and any one of the neighbors on the segment goes down, all routing updates may be lost. The single adjacency is torn down and despite the fact that the output of the **show clns neighbors** command still shows the neighbors, routing stops because there are no adjacencies.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(18)S1 or Release 12.3(9b) when an adjacency goes down while it is still in the INIT state. The symptom occurs because the adjacency counter is incorrectly decremented. The symptom may also occur in other releases.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface that reports only one adjacency.

Alternate Workaround: Enter the **clear clns neighbors** command on the affected router.

Miscellaneous

- CSCdy03863

Symptoms: When the **bandwidth** command is removed from a subinterface, the subinterface does not automatically obtain the bandwidth that is configured on the main interface.

Conditions: This symptom is platform- and release-independent.

Workaround: There is no workaround.

- CSCee20451

Symptoms: A VC may experience an output stuck condition.

Conditions: This symptom occurs when using T1 ATM (the IMA function is not used) on a PA-A3-8T1IMA.

Workaround: Perform the **clear interface** command.

- CSCeg07617

Symptoms: The following error message and spurious memory access may be generated on a Cisco 7500 series or Cisco 7600 series that is configured for dMLFR.

```
%ALIGN-3-SPURIOUS: Spurious memory access made at 0x418FC0E0 reading 0x8
%ALIGN-3-TRACE: -Traceback= 418FC0E0 4026B644 40699284 40699A3C 40699368 40E80B84
40E7215C 4068A8AC
```

Conditions: This symptom is observed immediately after an MFR interface is created, after a switchover has occurred, or when a link flaps continuously.

Workaround: There is no workaround.

- CSCeh15822

Symptoms: When a bandwidth is statically configured on a subinterface and when the subinterface is deleted and then recreated, the previously configured bandwidth statement may reappear under the subinterface configuration. When the subinterface is deleted, the following message is generated:

Not all config may be removed and may reappear after reactivating the sub-interface

Conditions: This symptom is platform- and release-independent.

Workaround: Verify the subinterface configuration upon recreation, and remove or reconfigure the configuration as needed.

- CSCei05246

Symptoms: After an OIR of a PA-MC-E3 port adaptor that is installed in a VIP6-80, the serial interfaces do not transmit. The message “not transmitting” is generated, followed by “output frozen.” After these messages, a Cbus Complex occurs.

Conditions: This symptom is observed on a Cisco 7500 series.

Workaround: There is no workaround.

- CSCej15698

Symptoms: The output of the **show ip mroute vrf vrf-name active** command shows an incorrect entry or rate for decapsulated traffic.

Conditions: This symptom is observed on a Cisco 12000 series that is configured for mVPN.

Workaround: There is no workaround.

- CSCej35894

Symptoms: Tracebacks are generated when you configure the card type for a clear channel T3/E3 Engine 5 SPA.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S3 or Release 12.0(32)S.

Workaround: There is no workaround.

- CSCej40549

Symptoms: A primary SR-APS physical interface may flap for several minutes in a scaled configuration with 1000 VCs that are configured while the router boots.

Conditions: This symptom is observed on a Cisco 12000 series that runs the c12kprp-p-mz image, that is configured with a 4-port OC-3 ATM ISE line card or 4-port OC-12 ATM ISE line card, and that has SR-APS enabled.

Workaround: There is no workaround.

- CSCej57949

Symptoms: When you change the Cisco IOS software image from any release to a release later than Release 12.0(27)S2, the redundancy mode is unexpectedly changed from SSO or RPR+ to RPR.

For example, the symptom occurs in the following situations:

- From Release 12.0(26)S4 to Release 12.0(31)S
- From Release 12.0(29)S to Release 12.0(31)S
- From Release 12.0(31)S to Release 12.0(28)S

Conditions: This symptom is observed on a Cisco 7500 series. The symptom does not occur when you change the Cisco IOS software image from any release to a release earlier than Release 12.0(27)S2. For example, the symptom occurs in the following situations:

- From Release 12.0(31)S1 to Release 12.0(26)S4
- From Release 12.0(27)S to Release 12.0(25)S

Workaround: After you have changed the Cisco IOS release, manually change the redundancy mode back from RPR to SSO or RPR+.

- CSCek05730

Symptoms: A Cisco 7200 series that runs Cisco IOS Release 12.0(31)S1 may crash unexpectedly because of a bus error and/or display some spurious memory accesses.

Conditions: This symptom is observed when an interface that is configured for some form of fancy queueing (that is, anything besides FIFO queueing) actively forwards traffic.

Workaround: Disable fancy queueing on the Ethernet interface.

- CSCek24821

Symptoms: The memory of a SIP-400 depletes entirely, and the following error message is generated:

```
EE48-3-ALPHA_MCAST: Can't assign new hw_mdb - (S,G)=(<IP>), mi=431, side=TX
```

Conditions: This symptom is observed on a Cisco 12000 series that functions as a PE router when the following conditions are present:

- The router receives traffic with invalid sources, that is the traffic is sent from sources that are not in the global routing table, causing RPF to fail.
- (S,G) information is still created for the invalid sources, and when the (S,G) information times out, the memory of the SIP-400 is not released.
- Regular traffic comes from a valid source and is directed to the same group address.
- The non-RPF source has a hash collision with the valid traffic stream.

Workaround: There is no workaround.

- CSCek25127

Symptoms: There is no IPv4 BGP MPLS functionality between BGP peers.

Conditions: This symptom is observed on a Cisco 12000 series that is connected to a BGP peer over a link bundle interface.

Workaround: There is no workaround.

- CSCek25442

Symptoms: MFR interfaces may flap on a Cisco 12000 series.

Conditions: This symptom is observed when a high rate of packets are punted to the CPU of the line card that is configured for low-priority Raw Queue (RawQ).

Workaround: Identify the reason for the high rate of packets that are punted to the CPU of the line card and correct the situation.

- CSCin74934

Symptoms: A VIP may crash when the MTU is changed on an MFR interface or on its member links.

Conditions: This symptom is observed on a Cisco 7500 series that is configured for dMFR.

Workaround: There is no workaround.

- CSCin79691

Symptoms: QoS information disappears from a FlexWAN module or VIP that is configured with a distributed MFR interface.

Conditions: This symptom is observed after the FlexWAN module or VIP resets or after the interface flaps.

Workaround: Remove the service policy from the interface and reapply it to the interface.

- CSCin86070

Symptoms: Polling the port speed (ifSpeed) for a subinterface returns a speed of 100 Mbps, which is incorrect.

Conditions: This symptom is observed on a 12000 series that is configured for MFR.

Workaround: Do not poll the ifSpeed of the subinterface. Rather, poll the ifSpeed of the main interface.

- CSCin95125

Symptoms: dCEF switching does not function when Frame Relay over L2TPv3 is configured on a 2-port OC-3 POS port adapter (PA-POS-2OC3) that is installed in a VIP 6-80.

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(30)S3 when an interface of the PA-POS-2OC3 faces the core of the network. When traffic from the core leaves the PA-POS-2OC3 to a CE router, dCEF switching functions fine. However, when traffic from the CE router leaves the PA-POS-2OC3 to the core, dCEF switching does not function and the VIP 6-80 punts the traffic to the RSP.

Workaround: There is no workaround.

- CSCin97815

Symptoms: Counters in the output of the **show policy-map interface mfr** command do not increment for any type and/or class of service. Even the class default shows no packets. The counters in the output of the **show frame-relay pvc** command show the packets correctly.

Conditions: This symptom is observed when a map class is configured on a subinterface that is part of an MFR (FRF.16) bundle and when the map class consists of both an input and output service policy.

Workaround: There is no workaround.

- CSCsa65822

Symptoms: Traffic from an Engine 3 or Engine 5 line card to an egress line card that is installed in slot 0 stalls.

Conditions: This symptom is observed on a Cisco 12000 series when you insert a new line card and remove the line card before it reaches the "IOS RUN" state, for example, when the line card is still in the "IOS STRT" or "IOS UP" state.

Workaround: After you have inserted a line card, wait until the line card is in the "IOS RUN" state before you remove it. If the line card becomes stuck before reaching the "IOS RUN" state, remove the line card, and enter the **show controller tofab queue 0** command on other Engine 3 or Engine 5 line cards in the chassis to check if the tofab queues towards slot 0 are uncorrupted. If the queues are corrupted, reload slot 0 to recover from the situation.

- CSCsb65210

Symptoms: A SIP does not accept the **show controller fia** command when you enter the command either via the **execute-on slot slot-number show controller fia** command or directly via the console of the line card, and a "% Incomplete command" message is generated.

Conditions: This symptom is observed on a Cisco 12000 series.

Workaround: There is no workaround.

- CSCsb88907

Symptoms: A Cisco 12000 series RP crashes when you enter the **clear l2tun all** command.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(30)S3 when the **debug vpdn l2x-packets** command is enabled on the router.

Workaround: Do not enter the **clear l2tun all** command when the **debug vpdn l2x-packets** command is enabled on the router.

- CSCsc30648

Symptoms: A POS line card that is configured with third-party vendor Small Form-Factor Pluggable Interface Converters (SFPs) and that is installed in a Cisco 12000 series fails the security check.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(30)S3 or Release 12.0(31) during the initial boot process.

Note that when the router runs Release 12.0(28)S3 and you boot the router with the SFPs already installed, the symptom does not occur. However, when you reload the router and then remove and reinsert the SFPs, they do not pass the security check either.

Workaround: There is no workaround.

- CSCsc52645

Symptoms: When Bit error rate testing (BERT) is configured on a timeslot or channel group, the entire T1 line goes down.

Conditions: This symptom is observed on a Cisco 7600 series and Cisco 12000 series that are configured with a channelized T3 to DS0 SPA.

Workaround: There is no workaround.

- CSCsc58216

Symptoms: When a VIP has an MLP bundle interface that is configured for LFI via the **ppp multilink interleave** command, counters on the bundle interface may show zero values, even when traffic is being passed.

Conditions: This symptom is observed on a Cisco 7500 series.

Workaround: Disable LFI by entering the **no ppp multilink interleave** command, or look at the counters for the physical interface.

- CSCsc65393

Symptoms: A 4-port Gigabit Ethernet ISE line card may crash.

Conditions: This symptom is observed on a Cisco 12000 series that is configured for multicast traffic.

Workaround: There is no workaround.

- CSCsc73112

Symptoms: On a Cisco 10000 series 4-port OC-3 ATM line card, a flowbit offset mismatch may occur on certain PVCs when you enter the **shutdown** interface configuration command on an ATM subinterface before you remove a service policy from the ATM subinterface.

Conditions: The symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.0(30)S4 and that is configured with a PRE1 when about 400 PVCs are activated on the line card.

Workaround: Do not enter the **shutdown** interface configuration command on the ATM subinterface before you remove the service policy.

- CSCsc80380

Symptoms: When you configure a class policer in a child policy by entering the **police cir percent** command, the police rate calculation for the class may be incorrect.

Conditions: This symptom is observed on a Cisco 12000 series that has an hierarchical Modular QoS CLI (MQC) output service policy on the Ethernet interface of a shared port adapter (SPA).

Workaround: Configure the police rate explicitly in bits-per-second.

- CSCsc88057

Symptoms: Traffic forwarding stops on the Gigabit Ethernet modular baseboard (EPA-GE/FE-BBRD) of a Modular GbE Engine 4+ line card.

Conditions: This symptom is observed on a Cisco 12000 series when you add an ACL to the 3-port Gigabit Ethernet port adapter (EPA-3GE-SX/LH-LC) of the same Modular GbE Engine 4+ line card.

Workaround: Perform a microcode reload on the 3-port Gigabit Ethernet port adapter of the Modular GbE Engine 4+ line card. Alternately, reload the router. However, note that both workarounds interrupt the traffic flow.

- CSCsc88940

Symptoms: After an RPF interface change occurs, the RPF check passes always on port 0 of an Engine 2 line card. This situation causes non-RPF traffic to be forwarded via the RPF interface and causes multicast traffic with a valid RPF (S,G) to be duplicated.

Conditions: This symptom is observed on a Cisco 12000 series and occurs because of an error during the calculation of the RPF interface.

Workaround: Do not use port 0 of an Engine 2 line card for multicast traffic in a configuration in which RPF interface changes may occur in such a way that port 0 receives non-RPF traffic.

- CSCsc96691

Symptoms: L2TPv3 traffic may not recover.

Conditions: This symptom is observed on a Cisco 12000 series after you have deleted and added a VLAN subinterface on a 4-port Gigabit Ethernet ISE line card (4GE-SFP-LC).

Workaround: Reload the router.

- CSCsd02954

Symptoms: Some CEF entries are missing from some VRFs, as shown in the output of the **show ip cef inconsistency now** command.

Conditions: This symptom is observed after an OIR or reload of a Cisco 12000 series GE ISE line card.

Workaround: There is no workaround. When the symptom has occurred, enter the **clear ip cef epoch** command to recover the CEF entries. If this does not recover the CEF entries, enter the **clear ip route vrf** command.

Further Problem Description: So far, the symptom is observed for local “receive” entries, such as /32 entries for a VRF loopback interface. However, the symptom may also occur for other types of VRF FIB entries.

- CSCsd03412

Symptoms: When you load a Cisco IOS software image, the interface-level uRPF configuration may be lost.

Conditions: This symptom is observed on a Cisco 12000 series when the uRPF interface level configuration has the **allow-self ping** keyword enabled in a command such as the **ip verify unicast source reachable-via allow-self-ping** command before you the Cisco IOS software image.

A list of the affected releases can be found at

<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd03412>. Cisco IOS software releases that are listed under the “All affected versions” link at this location are affected. Cisco IOS software releases that are listed in the “First Fixed-in Version” field at this location are not affected.

Workaround: To prevent the symptom from occurring, remove the **allow-self ping** keyword before you load the Cisco IOS software image. When the symptom has occurred, reconfigure each interface that lost the uRPF configuration and ensure that the **allow-self ping** keyword is not part of a command.

- CSCsd11701

Symptoms: When multicast hardware acceleration is enabled, a wrong label stack may be imposed on packets that have an IP destination address below 16.x.x.x. This situation occurs, for example, when the IP destination address is 10.1.1.1 and when the ingress interface is an MPLS VPN VRF subinterface that is configured for 802.1q. Note that in this situation, the CEF forwarding information is correct, that is, it has the correct label stack.

Conditions: This symptom is observed on a Cisco 12000 series that is configured with a 3-port GRE Engine 2 line card but may occur on any Engine 2 line card that has VRF interfaces. The symptom occurs only when multicast hardware acceleration is enabled.

A list of the affected releases can be found at

<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCei01644>. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

Workaround: There is no workaround.

- CSCsd18361

Symptoms: On a subinterface of a 4-port Gigabit Ethernet ISE line card (4GE-SFP-LC) that has an LDP neighborship with a neighbor that uses per-interface label space, when the LDP neighborship goes down, the subinterface stops forward traffic.

Conditions: This symptom is observed on a Cisco 12000 series. The symptom does not occur with a 3-port Gigabit Ethernet line card (3GE-GBIC-SC).

Workaround: There is no workaround.

- CSCsd23362

Symptoms: When MLP interfaces on a 1-port channelized OC-12/STM-4 (DS1/E1) ISE line card are configured for MVPN and you reload the router, the PIM VRF neighbor may not be established via a tunnel for some MLP interfaces.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(30)S4.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected MLP interfaces.

- CSCsd24601

Symptoms: The FIB becomes disabled when you bring down a member link of an MLP or MFR bundle.

Conditions: This symptom is observed on a Cisco 7500 series that is configured with an MLP or MFR bundle and that runs Cisco IOS Release 12.0(30)S, Release 12.0(31)S, or Release 12.0(32)S, all of which integrate the fix for caveat CSCeg57219. Other Cisco IOS software releases that integrate the fix for caveat CSCeg57219 are not affected.

Workaround: There is no workaround.

- CSCsd28415

Symptoms: When only one T1 link in a MLP bundle is active while all other links are shut down, the bundle does not pass traffic unless you bring up at least one more T1 link in the bundle.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S2.

Workaround: Bring up a second T1 link in the MLP bundle.

- CSCsd30704

Symptoms: When you first enter the **router isis area-tag** command followed by the **address-family ipv6** command and then change the administrative distance for the address-family IPv6 configuration, the RP may crash.

Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of Cisco IOS Release 12.0(30)S5, Release 12.0(31)S3, or Release 12.0(32)S1. The symptom may also occur on other platforms.

Workaround: There is no workaround.

- CSCsd38657

Symptoms: An RP crashes when a Gigabit Ethernet interface of a SPA is shut down. When this situation occurs, the following error message and traceback is generated:

```
Unexpected exception to CPUvector 700, PC = 2CEE34
-Traceback= 2CEE34 4C40000 2D8958 2D8D2C 2C1164 14048C 2CFB4C
```

If a crashinfo file is generated, the last log message is the following:

```
%SYS-6-STACKLOW: Stack for process CEF process running low, 0/6000
```

On a router that is configured with two RPs that function in RPR+ mode, when the RP crashes, a switchover occurs. However, the crashed RP does not come up and remains in standby mode.

Conditions: These symptoms are observed on a Cisco router when the recursive lookup on a static MPLS route does not specify a next hop interface. For example, the symptom occurs when the **ip route destination-prefix mask next-hop1** command is enabled but does not occur when the **ip route destination-prefix mask interface1 next-hop1** command is enabled.

Workaround: Ensure that the *interface* argument is included in the static route, as in the following command: **ip route destination-prefix mask interface1 next-hop1**.

Wide-Area Networking

- CSCsc76188

Symptoms: Even though the **show connection** command may indicate that an MFR segment is in the UP state, when you enter a more detailed command such as the **show connection id ID** command, the connection state may show as INVALID and the segment states as unknown.

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(31)S2 and occurs for both Frame Relay and MFR connections but not for ATM connections. Note that the symptom does not occur on a Cisco 12000 series.

Workaround: There is no workaround.

- CSCsd11874

Symptoms: When you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on an MFR interface when the bundle links are down, the serial interfaces that are associated with the MFR interface remain in the IDLE state.

Conditions: This symptom is observed on a Cisco router that is configure for MFR.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on each serial interface that is associated with the MFR interface.

Resolved Caveats—Cisco IOS Release 12.0(31)S3

Cisco IOS Release 12.0(31)S3 is a rebuild of Cisco IOS Release 12.0(31)S. The caveats listed in this section are resolved in Cisco IOS Release 12.0(31)S3 but may be open in previous Cisco IOS releases. This section describes only severity 1, severity 2, and select severity 3 caveats.

Basic System Services

- CSCsb14371

Symptoms: A Cisco 7500 series may log the following error message even if no VIP is installed in slot 0:

```
%IPC_RSP_CBUS-3-NOHWQ: Hardware queue for card at slot 0 not found
```

Conditions: This symptom is observed after a crash of another VIP has occurred. Sometimes the symptom occurs when a VIP is installed in slot 0 but most of the time there is no VIP in slot 0 when the symptom occurs.

Workaround: There is no workaround.

- CSCsb98906

Symptoms: A memory leak may occur in the “BGP Router” process.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(26)S6, that is configured for BGP, and that has the **bgp regexp deterministic** command enabled.

Workaround: Disable the **bgp regexp deterministic** command.

Interfaces and Bridging

- CSCef49896

Symptoms: Packets that enter an interface that is configured for IP may not be switched via dCEF.

Conditions: This symptom is observed on a Cisco 7500 series.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface.

ALternate Workaround: If many interfaces are affected, reload all port adapters by entering the **microcode reload** command on the control plane of the RSP.

- CSCsc71286

Symptoms: The throughput is far below what you would expect on an MFR bundle that is configured on a 8-port multichannel T1/E1 PRI port adapter (PA-MC-8TE1+).

Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.0(31)S2 when the MFR bundle has four T1 links, three of which are shut down. When you generate 2.5 Mbps of traffic to congest the one active link, a throughput of about 37 kbps to 59 kbps is observed. You would expect a throughput of about 1.5 Mbps.

Workaround: There is no workaround. The symptom does not occur in Release 12.3.

IP Routing Protocols

- CSCec12299

Devices running Cisco IOS versions 12.0S, 12.2, 12.3 or 12.4 and configured for Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) or VPN Routing and Forwarding Lite (VRF Lite) and using Border Gateway Protocol (BGP) between Customer Edge (CE) and Provider Edge (PE) devices may permit information to propagate between VPNs.

Workarounds are available to help mitigate this vulnerability.

This issue is triggered by a logic error when processing extended communities on the PE device.

This issue cannot be deterministically exploited by an attacker.

Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080924-vpn.shtml>.

- CSCei13040

Symptoms: When an OSPF neighbor comes back up after a very fast (sub-second) interface flap, OSPF routes that are learned via the interface that flapped may not be re-installed in the RIB.

Conditions: This symptom is observed when the following two events occur:

- The interface flaps very quickly.
- The neighbor comes back up before the LSA generation timer expires.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface that flapped.

Alternate Workaround: Enter the **clear ip route *** EXEC command.

- CSCei75375

Symptoms: OSPFv3 may write zeros into single words of memory in the heap. Depending on what (if anything) is allocated at the address that is being cleared, the router may reload or fail in some other way.

Conditions: This symptom is observed only when an OSPFv3 process or area is unconfigured or when you enter the **clear ipv6 ospf process** command and when both of the following conditions are present:

- The area that is removed or the process that is cleared contains one or more non-self-originated type-4 LSAs.
- The router does not have an intra-area path to an ASBR that is described by the type-4 LSA.

Workaround: There is no workaround.

- CSCsa79783

Symptoms: Routes are lost from the global routing table when Incremental SPF (ISPF) is enabled and when an OSPF neighbor bounces.

Conditions: This symptom is observed when multiple equal cost paths exist between OSPF neighbors.

Workaround: To prevent the symptom from occurring, disable ISPF. When the symptom has occurred, enter the **clear ip route *** command to re-instate the route.

- CSCsb36755

Symptoms: When BGP receives an update that has a worse metric route than the previously received route for equal-cost multipath, the BGP table is updated correctly but the routing table is not, preventing the old path from being deleted from the routing table.

Conditions: This symptom is observed on a Cisco router that is configured for BGP multipath.

Workaround: Enter the **clear ip route** *network* command.
- CSCsc36517

Symptoms: A router reloads unexpectedly when a continue statement is used in an outbound route map.

Conditions: This symptom is observed on a Cisco router that is configured for BGP.

Workaround: There is no workaround.
- CSCsc73436

Symptoms: High CPU usage may occur and the table versions of BGP peers are reset to zero.

Conditions: This symptom is observed when you update a complex policy on a Cisco router that has a complex configuration of BGP peers.

Workaround: There is no workaround.
- CSCsc75426

Symptoms: A router that is configured for BGP and that has the **ip policy-list** command enabled may unexpectedly reload because of a bus error or SegV exception.

Conditions: This symptom is observed when BGP attempts to send an update with a “bad” attribute.

Workaround: There is no workaround.

ISO CLNS

- CSCei04683

Symptoms: A router may advertise an IPv6 default route into a level-2 topology.

Conditions: This symptom is observed when the following conditions are present:

 - The router runs the IS-IS routing protocol on both level 1 and level 2.
 - The router advertises IPv6 prefixes.
 - The router has the IS-IS ATT bit set.
 - The router has level-1 connectivity to another level-1/level-2 IS-IS router.
 - An SSO switchover occurs on the router or the router loses and then regains connectivity to the level-2 topology.

Workaround: Trigger a change that causes the router to regenerate its level-2 LSP.
- CSCsb34032

Symptoms: A router may reload unexpectedly when you remove the IS-IS configuration at the interface or router level.

Conditions: This symptom is observed on a Cisco router when the following conditions are present:

 - The router is HA-capable.
 - The **isis protocol shutdown** interface configuration command is enabled on the interface.

- You enter an interface configuration command that enables IS-IS such as an **isis** command, a **clns** command, or the **ipv6 router isis** before you enter the a router configuration command such as the **net** command.

When you now remove the IS-IS configuration at the interface or router level, the router may reload.

Workaround: Remove the **isis protocol shutdown** interface configuration command before you remove IS-IS from the interface or router level.

Miscellaneous

- CSCeg24422

Symptoms: Packet drops occur in the ingress direction on a dMPLP or dMLFR link with traffic at 95-percent of the line rate and when the number of packets with a small size is high.

Conditions: This symptom is observed on a Cisco 7500 series that functions as a provider edge (PE) router, that is configured for L2TPv3 L3VPN, and that has dMPLP or dMLFR links to a customer edge (CE) router.

Workaround: There is no workaround.

- CSCeg57219

Symptoms: You cannot ping with packets of certain sizes after an RPR+ switchover or after an interface flap on a multilink interface that has members of non-channelized port adapters when the multilink interface is configured with fragmentation and interleaving.

Conditions: This symptom is observed on a Cisco 7500 series and Cisco 7600 series.

Workaround: There is no workaround.

- CSCeg76795

Symptoms: L2TPv3 sessions are re-established after their L2TP class has been deleted.

Conditions: This symptom is observed when you enter the **no l2tp-class** global configuration command to delete the class that is used by existing Xconnect paths via a pseudowire class.

Workaround: Remove the Xconnects paths along with the L2TP class.

- CSCeh32706

Symptoms: An inter-AS TE LSP fails to send a signal after a router is rebooted as an ASBR.

Conditions: This symptom is observed when there are parallel links between ASBRs with a combination of point-to-point and broadcast interfaces that are configured with the MPLS Traffic Engineering--Inter-AS TE feature and (passive) link flooding.

Workaround: Shut down the broadcast interface between the ASBRs.

- CSCeh62351

Symptoms: A router or line card may reload when you enter any of the following commands:

On a Cisco 7304:

- **show tech-support** command.
- **show hw-module subslot all status** command.
- **show hw-module subslot slot-number/subslot-number status** command.

On a Cisco 7600 series or Cisco 12000 series:

- **show tech-support** command.
- **show hw-module subslot all status** command.

- **show hw-module subslot *subslot-number* status** command.

Conditions: This symptom is observed when you enter above-mentioned commands on the console of a Cisco 7304 or on the console of a line card on a Cisco 7600 series or Cisco 12000 series when these routers are configured with any of the following SPAs (some SPAs are specific to the Cisco 7304 and some to the Cisco 12000 series):

- 2-port Gigabit Ethernet SPA
- 4-port FE SPA
- CT3 SPA
- T1/E1 SPA
- T3/E3 SPA

Workaround: There is no workaround.

- CSCeh63002

Symptoms: Service connections that are established with the **xconnect** command fail intermittently.

Conditions: This symptom is observed with both large configurations (with more than 4000 Xconnect service connections) and medium configurations (with 1000 Xconnect service connections) when several changes such as OIRs or dynamic reconfigurations occur. The symptom is intermittent and very unlikely to occur in small configurations, and it is unlikely to occur in large configurations that do not undergo changes.

Workaround: There is no workaround. You must re-establish the service connections by re-entering the **xconnect** command.

- CSCeh80649

Symptoms: When a T3 line flaps, the serial interface that is configured on the T1 channel group (over the T3 line) may fail to come up and may stay in the “Line Protocol down” state.

Conditions: This symptom is observed on a Cisco 7600 series and Cisco 12000 series that are configured with a channelized T3 to DS0 SPA or 1-port channelized STM-1/OC-3 SPA that is configured with channelized T1 serial interfaces.

Workaround: Reload the SPA by entering the **hw-module subslot *slot/subslot* reload** command.

- CSCeh85133

Symptoms: A memory leak may occur when an SNMP trap is sent to a VRF destination. The output of the **show processes memory** command shows that the memory that is held by the process that creates the trap increases, and eventually causes a MALLOC failure. When this situation occurs, you must reload the platform.

Conditions: This symptom is platform-independent and occurs in a configuration in which at least one VRF destination has the **snmp-server host** command enabled.

Workaround: Ensure that no VRF is associated with the **snmp-server host** command.

- CSCeh90984

Symptoms: When you enter the **clear cef linecard** command, CEF may be disabled on a POS ISE line card and does not recover by itself.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S3.

Workaround: Reload the line card.

- CSCei01644

Symptoms: A 3-port Gigabit Ethernet (3GE-GBIC-SC) line card that is configured for Fast-Path Multicast Forwarding may reset when receiving specific packets. However, it is not necessary that the line card will crash all times. The resulting action on these packets could result in a simple drop as well.

Conditions: This symptom is observed on a Cisco 12000 series when a packet with an IP destination address from the reserved multicast range (224.0.0.xxx) and a TTL larger than 1 is received on the 3GE-GBIC-SC line card and when multicast hardware acceleration is enabled.

Normally, the TTL should be 1 if the destination address is part of the reserved multicast range.

Workaround: Enter the **no hw-module slot *slot-number* ip multicast hw-accelerate source-table size 16 offset 0** command.

- CSCei24302

Symptoms: When traffic enters an Engine 6 ingress interface and flows in the direction of equal-cost multiple egress interfaces, all traffic is lost.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(27)S5, Release 12.0(28)S3, or Release 12.0(31)S when the traffic destination is present in the routing table as a recursive route (for example, learned via iBGP) and when the router has the IP Source Tracker feature configured. The symptom occurs only when the ingress interface is an interface of an Engine 6 link card and when multiple equal-cost egress interfaces are used.

Workaround: Enter the **clear ip route *** command to enable the traffic to reach its destination.

- CSCei30764

Symptoms: A PE router that is configured with many (100 or more) Multicast VRFs (mVRFs) may create multiple MDT tunnels for one mVRF.

Conditions: This symptom is observed when you reload a Cisco router that functions as a PE router and that is configured for MVPN.

Workaround: There is no workaround.

- CSCei33598

Symptoms: A T3 controller of a channelized T3 to DS0 SPA stays down when the remote router reloads or when the loopback interface is enabled or disabled.

Conditions: This symptom is observed on a Cisco 7600 series and Cisco 12000 series that have T1 FDL transmission enabled and occurs because unterminated FDL packets exist. The symptom does not occur when the T1 FDL transmission is disabled.

Workaround: Disable T1 FDL transmission on both ends.

- CSCei36672

Symptoms: Interfaces on a 1-port 10-Gigabit Ethernet Engine 5 SPA remain administratively shut down.

Conditions: This symptom is observed on a Cisco 12000 series after an RPR Plus (RPR+) switchover has occurred.

Workaround: Prevent an RPR+ switchover from occurring. If this is not an option, there is no workaround.

- CSCei54336

Symptoms: An MPLS LER does not impose labels for traffic that follows the default route, causing traffic to be forwarded via IP.

Conditions: This symptom is observed on a Cisco 12000 series when the default route has two equal paths, when the ingress line card is an ISE line card, and when the default router is learned via OSPF. The symptom may also occur for other protocols.

Workaround: Use a single path for the default route. If this is not an option, there is no workaround.

- CSCei62762

Symptoms: Router may generate and/or forward crafted IP packets with the source IP address being the routers tunnel interface for GRE or mGRE tunnels. Incorrect packet decoding may be seen with “debug tunnel.”

Conditions: The router needs to receive a specially crafted GRE packet sent to the tunnel end-point. The outer IP packet must come from the configured tunnel source and be sent to the configured tunnel destination IP address Present Routed bit must be set to 1.

Workaround: Upgrade Cisco IOS to a version containing fixes for: CSCuk27655 or CSCea22552 or CSCei62762.

Further information: On the 6th September 2006, Phenoelit Group posted an advisory:

* Cisco Systems IOS GRE decapsulation fault

Cisco’s statement and further information are available on the Cisco public website at:

<http://www.cisco.com/warp/public/707/cisco-sr-20060906-gre.shtml>

- CSCei69875

Symptoms: Hardware multicast forwarding does not function.

Conditions: This symptom is observed on a Cisco 12000 series after you have reloaded the router.

Workaround: Remove and re-apply hardware multicast forwarding.

- CSCei84343

Symptoms: IP packets that are forwarded from an Engine 6 interface on a Cisco 12000 series to an iBGP route may not reach the destination node.

Conditions: This symptom is observed when the Engine 6 interface forwards these packets as IP packets even though there is a labeled path to the BGP next hop. The output of the **show cef** command shows that the router uses the MPLS labeled path but the Engine 6 hardware is programmed to forward the packets as IP packets instead of MPLS packets. The next router that receives these IP packets may drop them because the next router may be unaware of the iBGP route.

Workaround: There is no workaround.

- CSCei93119

Symptoms: CEF may become disabled on an Engine E4+ line card because of a MALLOC failure.

Conditions: This symptom is observed on a Cisco 12000 series when you enter the **no mpls ip** global configuration command immediately followed by the **mpls ip** global configuration command.

Workaround: There is no workaround.

- CSCei94758

Symptoms: After an APS switchover, end-to-end traffic does not recover.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)SA4 and that is configured with redundant PRPs that run in RPR+ mode during a Large Scale Network Test (LSNT). The router has two channelized OC-12 line cards that are configured for APS and that each have 280 DS1 ports, 121 DS0 ports, and 42 MLP groups.

Workaround: There is no workaround.

- CSCei95220

Symptoms: When an APS switchover occurs on 1-port channelized ISE line cards, traffic may not recover although the controllers may be in up state. The interfaces may remain indefinitely in the up/down state.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S or an earlier release when a significant amount of traffic is being processed when the APS switchover occurs.

Workaround: There is no workaround. However, the built-in failure detection mechanism detects that the ingress data path is locked up and automatically resets the PLIM of the affected line card.

- CSCej01615

Symptoms: On a router that is configured for Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP), the CPU usage may increase considerably for an extended period of time when a large number of label bindings are withdrawn or released at the same time.

Conditions: This symptom is observed on a Cisco router only when LDP (as opposed to TDP) is used and when a large number (more than 250) of LDP neighbors and a large number of IP prefixes become unreachable at the same time.

Workaround: There is no workaround.

- CSCej04699

Symptoms: The output of the **show ip hardware-cef tofab prefix** command may display incorrect information for Engine 5 line cards.

Conditions: This symptom is observed on a Cisco 12000 series that functions in a scaled routing environment with more than 100,000 routes.

Workaround: There is no workaround.

- CSCej07539

Symptoms: Multicast traffic does not resume fully after you have removed the active PRP from the router.

Conditions: This symptom is observed on a Cisco 12000 series that runs the c12kprp-p-mz image of Cisco IOS Release 12.0(28)S4 and that is configured with redundant PRPs that function in RPR+ mode. The router has two channelized OC-12 line cards that are configured with mVPNs.

Workaround: There is no workaround.

- CSCej09368

Symptoms: On an Ethernet over AToM link, an abnormal queue depth may occur for Time-Based WRED and Byte-Based-WRED.

Conditions: This symptom is observed on a Cisco 7500 series but is platform-independent.

Workaround: There is no workaround.

- CSCej10404

Symptoms: Fast Reroute (FRR) fails on a remote provider (P) router, causing packet loss.

Conditions: This symptom is observed on a Cisco 12000 series that functions as a P router in the following topology:

- One P router (P1) connects to another P router (P10) via a primary tunnel that is configured on a 1-port 10-Gigabit Ethernet Engine 5 SPA. (P10 functions as the tunnel head-end.)
- There is a backup next-hop (NHOP) FRR protection tunnel via an LSP path between P1 and P10.

- P1 connects also to another P router (P2) that connects to yet another P router (P3), that, in turn, connects to P10, forming a second backup NHOP FRR protection tunnel via an LSP path.

When the link between P1 and P10 breaks at P1, the secondary backup tunnel does not come up immediately, causing packet loss of around 200 ms (about 90 percentile) when the link goes down and 5 seconds when the link finally comes up again.

Workaround: Enter the **mpls traffic-eng topology holddown sigerr 0** command on the affected tunnel head-end (P10) to prevent the backup LSP from being hold down.

Further Problem Description: This symptom is only observed with 1-port 10-Gigabit Ethernet Engine 5 SPAs.

- CSCej14847

Symptoms: Auto-RP messages from a CE router are lost.

Conditions: This symptom is observed when you enter the **clear ip mroute *** on a connected PE router. The messages do not recover by themselves.

Workaround: To restart Auto-RP messages, enter the **clear ip mds linecard** command.

Alternate Workaround: To restart Auto-RP messages, debug the VRF Auto-RP by entering the **debug ip pim vrf vrf-name auto-rp**.

- CSCej32588

Symptoms: An interface of an Engine 6 line card is no longer shut down after an RP switchover occurs.

Conditions: This symptom is observed on a Cisco 12000 series when the following events occur:

1. The interface of the Engine 6 line card is configured with the **no shutdown** interface configuration command in the startup configuration.
2. The router is reloaded and you verify that the interface comes up.
3. You enter the **shutdown** interface configuration command on the interface.
4. You enter the **write memory** command.
5. You enter the **redundancy force** command.

After the new RP comes up, the interface appears no longer shut down and the interface comes up again.

Workaround: After you have entered the **shutdown** interface configuration command on the interface followed by the **write memory** command, reload the router.

- CSCej42144

Symptoms: A service policy on an Engine 4 + or Engine 6 line card is incorrectly rejected with the following error message:

```
%E4P and E6 LC requires to configure POLICE and SET %command in every class if either of these two commands %is configured in class-default class
```

This situation occurs when a **set** command is used in all classes.

Conditions: This symptom is observed on a Cisco 12410 that runs Cisco IOS Release 12.0(28)S3, that is configured with dual Performance Route Processors (PRP-1s) that operate in SSO mode, and that has multiple E4+ and/or Engine 6 line cards.

Workaround: There is no workaround.

- CSCej69557

Symptoms: After you reload a PE router that functions in an MVPN topology and that is configured for sparse mode and Auto-RP, the router may not learn the Auto-RP that is advertised by both a local and remote CE router, preventing traffic from resuming to flow.

Conditions: This symptom is observed on a Cisco 12000 series that runs an interim release for Cisco IOS Release 12.0(32)S and that functions as a PE router. The symptom may also occur in other releases of Release 12.0S.

Workaround: Enter the **clear ip mds line** command.

- CSCej82265

Symptoms: An MPLS TDP peer is down.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S3 and that has the **mpls ldp protocol tdp** command configured on the interface on which TDP peering cannot be established. The peer router has the **mpls ldp protocol both** command configured.

Workaround: Enter the **mpls ldp protocol tdp** command on the peer router. Note that this workaround may not be plausible for routers that run a legacy Cisco IOS software that only supports TDP.

- CSCej86009

Symptoms: The atmImaMibTraps SNMP trap returns the NOSUCHINSTANCE error for the imaAlarmType and imaAlarmStatus varbinds.

Conditions: This symptom is observed on a Cisco 7500 series but may be platform-independent.

Workaround: There is no workaround.

- CSCej86175

Symptoms: In a multicast VPN (MVPN) environment, when a Stateful Switchover (SSO) occurs on a PE router, the multicast traffic in the MVRF does not recover because the neighboring PE router fails to re-establish its PIM neighbor relationship. Note that the symptom does not occur for unicast traffic.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S2 or an interim release for Release 12.0(32)S and that functions as a PE router (PE1) in the following topology:

multicast origination --> PE2 --> PE1 --> CE1 --> multicast termination

When an SSO occurs on PE1, PE2 does not re-establish its PIM neighbor relationship with PE1 in the MVRF. PE1 and PE2 are global PIM neighbors.

Workaround: Reload PE1.

Further Problem Description: When the symptom occurs, PE1 still shows PE2 as its PIM neighbor in the MVRF. Clearing the multicast route in the MVRF does not help to resolve this issue.

- CSCek08638

Symptoms: Data traffic that is received by a provider edge (PE) router on an Ethernet port may not be forwarded over an L2TPv3 tunnel.

Conditions: This symptom is observed on a Cisco 12000 series when the line card that faces the customer edge (CE) router is one of the following line cards:

- 8-port Fast Ethernet, 100BASE-FX line card (8FE-FX-SC-B)
- 8-port Fast Ethernet, 100BASE-TX line card (8FE-TX-RJ45-B)

- 1-port Gigabit Ethernet line card (GE-GBIC-SC-B)

Workaround: There is no workaround.

- CSCin79691

Symptoms: QoS information disappears from a FlexWAN module or VIP that is configured with a distributed MFR interface.

Conditions: This symptom is observed after the FlexWAN module or VIP resets or after the interface flaps.

Workaround: Remove the service policy from the interface and reapply it to the interface.

- CSCin91381

Symptoms: A VIP that has a dMLFR configuration may crash when you enter the **microcode reload** global configuration command.

Conditions: This symptom is observed on a Cisco 7500 series when traffic flows through the VIP.

Workaround: There is no workaround.

- CSCin96692

Symptoms: On a Cisco 7500 series that is configured for dMLP, the txacc values of member interfaces may be wrongly credited to other member interfaces, causing RSP-3-RESTART messages, and finally causing traffic to stop.

Conditions: This symptom is observed when the member links flap continuously for some time while traffic is being processed.

Workaround: There is no workaround.

- CSCsa70494

Symptoms: When the remote router is reloaded, the local router reports an error message such as the following one:

```
%SPA_CHOC_DSX-3-HDLC_CTRL_ERR: SPA 5/2: 6 TX Chnl Queue Overflow events on HDLC
Controller were encountered.
```

This situation causes some packets to become lost.

Conditions: This symptom is observed on a Cisco router that is configured with a channelized T3 to DS0 SPA when the following conditions occur:

- The SPA is configured with many multilink bundles.
- A heavy traffic load is being processed.
- Links go down at the remote end.

Workaround: Shut down the links on the channelized T3 to DS0 SPA before the router at the remote site is reloaded. If this is not an option, there is no workaround.

- CSCsa80620

Symptoms: Member links of a multilink bundle remain down, traffic does not flow, and an error message similar to the following is generated on the console of the RP and line card:

```
%C7600_SIP200_SPITX-3-EFC_QUEUE_STUCK: Se4/2/0/3:0
```

Conditions: This symptom is observed on a Cisco router and Cisco switch that are configured with a 2- or 4-port channelized T3 to DS0 SPA when a member link of a multilink bundle is directly added to another multilink bundle without first deleting the member link from the first bundle.

Workaround: First delete the member link from one multilink bundle before you add the member link to another multilink bundle.

To bring up the member links after the symptom has occurred, enter the **shutdown** controller configuration command followed by the **no shutdown** controller configuration command on the T3 controller of the SPA on which the multilink bundle is configured.

- CSCsa91478

Symptoms: A Cisco 12000 series that is configured for L2TPV3 may continuously log the following CM_ERROR message, causing the syslog server to be flooded:

```
%SW_MGR-3-CM_ERROR: Connection Manager Error - unprovision segment failed
%SW_MGR-3-CM_ERROR: Connection Manager Error - unprovision segment failed
```

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(30)S1 when a Multilink Frame Relay (MFR) interface is shut down in the configuration of the **connect** command, causing proper provisioning to fail, unprovisioning to occur, and the error message to be generated.

Possible Workaround: Enter the **no shutdown** interface configuration command on the MFR interface.

- CSCsb00473

Symptoms: A channelized T3 to DS0 SPA hangs and remains unresponsive.

Conditions: This symptom is observed on a Cisco router when you configure a large number of T1 links in SF framing mode simultaneously on channelized T3 to DS0 SPAs that are connected back-to-back.

Workaround: Do not do configure a large number of T1 links in SF framing mode simultaneously on channelized T3 to DS0 SPAs that are connected back-to-back. When the symptom has occurred, you must reload the affected SPA.

- CSCsb11124

The Cisco IOS Stack Group Bidding Protocol (SGBP) feature in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable denial of service condition. Devices that do not support or have not enabled the SGBP protocol are not affected by this vulnerability.

Cisco has made free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability.

Cisco has published a Security Advisory on this issue; it is available at <http://www.cisco.com/warp/public/707/cisco-sa-20060118-sgbp.shtml>.

- CSCsb12969

Symptoms: All VIPs or FlexWAN modules reload unexpectedly on a platform that is configured for Modular QoS CLI (MQC).

Conditions: This symptom is observed on a Cisco 7500 series (with VIPs) and a Cisco 7600 series and Cisco Catalyst 6500 series (both with FlexWANs) when the following steps occur while the physical interface is in the UP state:

1. An input policy and output policy map are already attached to an ATM or Frame Relay PVC. When you attach the same policy map to the main interface, an error message is generated and the configuration is rejected.
2. You remove the policy map from the PVC and attach the same policy map to the main interface.
3. You remove the policy map from the main interface.

At this point, all VIPS or FlexWAN modules reload, even though no traffic is being processed during the above-mentioned steps.

Workaround: There is no workaround.

- CSCsb25404

Symptoms: The startup configuration in NVRAM is not loaded onto line cards when the router is manually reloaded.

Conditions: This symptom is observed on a Cisco 12000 series that functions as a multiservice edge (MSE) router when the ATM Cell Relay over MPLS feature is configured on 500 connections. The symptom may also occur on other platforms.

Workaround: After the router has been reloaded, cut and paste the initially rejected configuration onto the line cards.

- CSCsb28139

Symptoms: An LDP/BGP adjacency is not formed, and a ping does not go through.

Conditions: This symptom is observed on a Cisco 12000 series that functions in a scaled VPN environment when an Engine 6 line card faces the core of the MPLS network.

Workaround: Enter the **clear ip route *** command.

- CSCsb38396

Symptoms: When a 2-port or 4-port channelized T3 to DS0 SPA is configured with MFR subinterfaces and when you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on one of the subinterfaces, the subinterface does not come up.

Conditions: This symptom is observed on a Cisco 12000 series.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the main interface to enable the subinterface to come up.

- CSCsb39165

Symptoms: A Cisco router may report high CPU usage and memory depletion under a specific MPLS VPN configuration with static routes.

Conditions: This symptom is observed when equal cost static routes to a subnet point to a next hop address and there is a summary route that covers one of the next hops pointing to Null0.

If the directly connected route to the next hop is terminated because the interface goes down, the original route recurses to Null0 while the route recursing through the interface that is still up remains in the routing table. The end result is that the route now points to both Null0 and to a valid interface that is up, causing an MPLS recursion problem that results in high CPU usage and memory depletion.

The following is an example configuration:

```
ip route a.a.a.a b.b.b.b y.y.y.y
ip route a.a.a.a b.b.b.b z.z.z.z
ip route y.y.y.y mask Null0
```

If the directly connected route y.y.y.y is removed the a/b subnet recurses through the y.y.y.y/mask route to Null0.

Workaround: Use routes that point to both a next hop and an egress interface, as in the following example:

```
ip route a.a.a.a b.b.b.b interfaceY y.y.y.y
ip route a.a.a.a b.b.b.b interfaceZ z.z.z.z
```

Workaround: There is no workaround.

- CSCsb46607

Symptoms: A standby route processor (RP) may crash in the “CEF LC IPC Background” process.

Conditions: This symptom is observed on a Cisco platform when an SSO switchover occurs.

Workaround: There is no workaround.
- CSCsb58311

Symptoms: An IMA port adapter may fail to receive data on a VC that is configured for cell packing with AAL0 encapsulation. The “ignored” counter in the output of the **show interface** command increments and the “rx_cell_throttle” count in the output of the **show controllers** command also increments.

Conditions: This symptom is observed when the Maximum Number of Cells Packed (MNCP) parameter is changed for a large number (around 100) of VCs.

Workaround: There is no workaround.
- CSCsb83876

Symptoms: The counters on a PA-MC-E3 port adapter may provide incorrect information. For some interfaces of the port adapter, the counters are always zero, and for others interfaces, the counters do increase but very slowly.

Conditions: This symptom is observed when you enter the **show interfaces type slot** command for a PA-MC-E3 port adapter.

Note that the symptom does not occur when you enter the **show interface type number stats** command or the **show interfaces type slot accounting** command. Also, when you enter the **show interfaces type slot** command for the VIP in which the PA-MC-E3 port adapter is installed, the counters provide correct information.

Workaround: Enter the **show interface type number stats** command to retrieve the correct information.
- CSCsb85338

Symptoms: When you perform an OIR of an alarm module or fan module, the inventory serial number (SN) may become lost after the new module is inserted, and the output of the **show inventory** command may not show the SN.

This situation prevents you from keeping track of the inventory and affects the operation of the Component Outage On-Line (COOL) feature.

Conditions: This symptom is observed on a Cisco 12000 series.

Workaround: There is no workaround.
- CSCsb98254

Symptoms: A router may fail when you reload a Gigabit Ethernet (GE) line card or port adapter that has link-bundling enabled.

Conditions: The problem may occur with dot1Q on the GE interface and MPLS enabled on some uplink. This symptom is observed on a Cisco 12000 series that runs a Cisco IOS interim release for Release 12.0(32)S and that is configured for MPLS. However, the symptom is platform-independent and may also occur in other releases.

Workaround: There is no workaround.
- CSCsc09436

Symptoms: An Engine 5 line card crashes when the Fabric MIB is polled.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S1 and only affects Engine 5 line cards.

Workaround: Create an SNMP View that excludes the Fabric MIB (CISCO-FABRIC-C12K-MIB).

- CSCsc30289

Symptoms: When the router at the opposite site is reloaded, a Dynamic Packet Transport (DPT) line card crashes because of a “Bus Error exception.”

Conditions: This symptom is observed on a Cisco 12000 series when the router at the opposite site is also configured with a DPT line card.

Workaround: There is no workaround.

- CSCsc32171

Symptoms: An Engine 2 line card that functions as a tunnel server card may crash in the process_rx_packet_util_inline() process when an Xconnect configuration is removed.

Conditions: This symptom is observed on a Cisco 12000 series when a dynamic L2TP session that is configured on a tunnel server card is removed while traffic is being processed.

Workaround: There is no workaround.

- CSCsc37404

Symptoms: An Engine 6 line card may reset with the following error messages:

```
%IPC-5-INVALID: NACK Source Port=0x403F0000
%MCC192-3-CPU_PIF: Error=0x4
%MCC192-3-CPUIF_ERR: Packet Exceeds Programmed Length.
%GSR-3-INTPROC: Process Traceback= 40D32E5C 406D8CE0
...
```

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S2.

Workaround: There is no workaround.

- CSCsc38678

Symptoms: When IS-IS IPv6 routes flap, a memory leak occurs on an ISE line card, eventually causing dCEF to be disabled when no more memory is available.

Conditions: This symptom is observed on a Cisco 12000 series that is configured with 180,000 BGP routes and 6000 IS-IS routes, 10 percent of which flaps each 30 seconds. The symptom occurs only when IS-IS flaps, not when BGP flaps. The symptom does not occur either when IPv6 routing is not configured.

Workaround: There is no workaround. If this is an option, remove IPv6 routing by entering the **no ipv6 unicast-routing** global configuration command. When the symptom has occurred and dCEF is disabled, you must reload the line card to restore its memory.

- CSCsc44237

This caveat consists of two symptoms, two conditions, and two workarounds:

1. Symptom 1: A switch or router that is either configured with a PA-A3 ATM port adapter may eventually run out of memory. The leak occurs when the FlexWAN or VIP that contains the PA-A3 port adapter is removed from the switch or router and not re-inserted.

The output of the **show processes memory** command shows that the “ATM PA Helper” process does not have sufficient memory. The output of the **show memory allocating-process totals** command shows that the “Iterator” process holds the memory.

Condition 1: This symptom is observed on a Cisco Catalyst 6500 series, Cisco 7500 series, and Cisco 7600 series.

Workaround 1: Either do not remove the PA-A3 ATM port adapter from the FlexWAN or VIP or re-insert the PA-A3 ATM port adapter promptly. The memory leak stops immediately when you re-insert the PA-A3 ATM port adapter.

2. Symptom 2: A switch or router that has certain PIM configurations may eventually run out of memory.

The output of the **show processes memory** command shows that the “PIM process” does not have sufficient memory. The output of the **show memory allocating-process totals** command shows that the “Iterator” process holds the memory.

Condition 2: This symptom observed on a Cisco 2811 and Cisco 3845 and occurs only in Cisco IOS Release 12.2(30)S, interim Release 12.4(2.10), and interim Release 12.4(2.10)T, or in any later releases.

Workaround 2: When the **ip multicast-routing** command is configured, enable at least one interface for PIM. When the **ip multicast-routing vrf vrf-name** command is configured, enter the **ip vrf forwarding vrf-name** command on at least one interface that has PIM enabled.

- CSCsc46474

Symptoms: When you create a VRF, a router generates the following error message for a link bundle that does support MPLS VPN and that is configured on a 3-port Gigabit Ethernet (GE) Engine 2 line card:

```
%LC-6-PSA_UCODE_NO_SUPPORT: Current bundle does NOT support (MPLS VPN)
```

When you apply the VRF to an interface of the 3-port GE Engine 2 line card by entering the **ip vrf forwarding** command, the 3-port GE Engine 2 line card crashes.

Conditions: These symptoms are observed on a Cisco 12000 series that is configured with a port channel for link bundling.

Workaround: There is no workaround.

- CSCsc50086

Symptoms: The output of the **show inventory** command for a SPA may not show the SPA inventory or the output may show an outdated SPA inventory.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S when you move the SIP in which the SPA is installed to another slot.

Workaround: There is no workaround.

- CSCsc53960

Symptoms: A spurious memory access error is generated when you enter the **connect** command to provision locally-switched ATM PVCs. The output of the **show alignment** command shows that the spurious access counter is incremented.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S2.

Workaround: There is no workaround.

- CSCsc54584

Symptoms: A standard ingress ACL for transit traffic does not function on an interface that is configured for MFR.

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.3(11)T8 and that has an MFR bundle that is configured on a PA-MC-8TE1 port adapter. The symptom may also occur in other releases.

Workaround: There is no workaround.

- CSCsc55477

Symptoms: When you regularly poll the ifHCInOctets MIB counter on a subinterface of a Modular GbE Engine 4 line card, the counter restarts at zero after the value 274651394019 (around 2^{38}) has been reached. The ifHCInOctets MIB counter is supposed to restart at zero after the value 2^{64} has been reached.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S2.

Workaround: There is no workaround. Note that the symptom does not occur in Release 12.0(28)S5.

- CSCsc58973

Symptoms: When the **mpls ping** and **traceroute** commands are configured, the specified destination address does not take effect, nor is the 127.0.0.1 default address used when the destination address is not specified. Instead, the target FEC is used as the destination IP address in IP header of the outgoing packet.

When you specify a range of destinations for troubleshooting, the target IP address is always used. This situation prevents you from using the **mpls ping** and **traceroute** commands to troubleshoot an equal-cost multipath (ECMP) configuration.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0S.

Workaround: There is no workaround.

- CSCsc63558

Symptoms: A 2-port OC-192 POS Engine 6 line card (the 2OC192/POS-SR-SC and the 2OC192/POS-IR-SC) may stop forwarding traffic after running properly for a while. When this situation occurs, the POS interface is in the UP/UP state, but a ping to the directly connected POS interfaces fails. No error messages are generated for the affected line card.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S2 or Release 12.0(28)S5, irrespective of whether or not an ACL is configured on the line card.

Workaround: There is no workaround. You must reset the line card to recover from the symptoms.

- CSCsc64723

Symptoms: After an SSO switchover, traffic does not fully recover on a 3-port GE Engine 2 line card that is configured for EoMPLS.

Conditions: This symptom is observed on a Cisco 12000 series that runs the c12kprp-p-mz image of Cisco IOS Release 12.0(28)S5.

Workaround: Enter the **clear cef linecard slot-number** command to recover from the symptom and enable traffic to pass properly.

- CSCsc82234

Symptoms: A multicast RPF check fails when the **maximum-paths eibgp** command is configured as part of an IPv4 VRF.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(31)S2 and that is configured for L2TPv3.

The symptom occurs because RPF expects the gateway for the VPNv4 route to be either in the same VRF or in the global routing table context, which is not the case when L2TPv3 is configured.

Workaround: Disable the **maximum-paths eibgp** command.

TCP/IP Host-Mode Services

- CSCsc39357

Symptoms: A Cisco router may drop a TCP connection to a remote router.

Conditions: This symptom is observed when an active TCP connection is established and when data is sent by the Cisco router to the remote router at a much faster rate than what the remote router can handle, causing the remote router to advertise a zero window. Subsequently, when the remote router reads the data, the window is re-opened and the new window is advertised. When this situation occurs, and when the Cisco router has saved data to TCP in order to be sent to the remote router, the Cisco router may drop the TCP connection.

Workaround: Increase the window size on both ends to alleviate the symptom to a certain extent. On the Cisco router, enter the **ip tcp window-size bytes** command. When you use a Telnet connection, reduce the *screen-length* argument in the **terminal length screen-length** command to 20 or 30 lines.

Further Problem Description: BGP in Cisco IOS Release 12.0S and Release 12.4 is not affected because the retransmit timeout is disabled for BGP in these releases.

Wide-Area Networking

- CSCsb61367

Symptoms: When you enter the **redundancy force-switchover** command on a router that is configured for PPP encapsulation, the IS-IS neighbor comes up in the INIT state.

Conditions: This symptom is observed on a Cisco router that is configured with two RPs that run in SSO redundancy mode.

Workaround: To bring up the IS-IS state in the IS-IS neighbor, enter the **isis protocol shutdown** interface configuration command followed by the **no isis protocol shutdown** interface configuration command on interface that provides the connection to the IS-IS neighbor.

Alternate Workaround: Configure HDLC encapsulation on the router.

- CSCsc52545

Symptoms: A VIP in which ATM port adapters are installed may crash.

Conditions: This symptom is observed on a Cisco 7500 series that is configured with two RPs that function in RPR+ mode.

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.0(31)S2

Cisco IOS Release 12.0(31)S2 is a rebuild of Cisco IOS Release 12.0(31)S. The caveats listed in this section are resolved in Cisco IOS Release 12.0(31)S2 but may be open in previous Cisco IOS releases. This section describes only severity 1, severity 2, and select severity 3 caveats.

Basic System Services

- CSCsb08386

Symptoms: A router crashes when you enter the **show ip bgp regexp** command.

Conditions: This symptom is observed on a Cisco router when BGP is being updated.

Workaround: Enable the new deterministic regular expression engine by entering the **bgp regexp deterministic** command and then enter the **show ip regexp** command. Note that enabling the new deterministic regular expression engine may impact the performance speed of the router.

- CSCdu32036

Symptoms: When applying an access-list for SNMP using the command:

```
snmp-server tftp-server-list
```

The access-list is not applied, so it is possible to copy the config to and from any server, regardless of the contents of the access-list.

Conditions: The SNMP service must be running for this defect to manifest itself.

The following sample configuration should cause the device to reject configuration file transfers via SNMP from all hosts except the TFTP server specified in access list 5:

```
!
!
snmp-server tftp-server-list 5
- --- cut ---
!
access-list 5 permit 10.1.1.1
snmp-server community private RW 5
snmp-server tftp-server-list 5
!
```

When this defect is present, the device will allow configuration file transfers from any server, regardless of the contents of the access-list.

Workaround:

- Disable the SNMP service.
- Apply a more general access list to restrict traffic to and from the affected device.

- CSCec75641

Symptoms: A Cisco router may reload when there are two or more Telnet or console sessions to the router.

Conditions: This symptom is observed when the following events occurs:

- In one session, enter the **show ip as-path-access-list acl-number** command. The output pauses at the “--more--” prompt when there is more than one page output.
- In another session, enter the **no ip as-path access-list acl-number** command in which the *acl-number* argument is the same one as in the **show ip as-path-access-list acl-number** command.
- In the first session, type in “enter” or “space” in the first session to display the rest of the show command output.

Workaround: Do not enter the **show ip as-path-access-list acl-number** command when the **no ip as-path access-list acl-number** command is being configured.

IP Routing Protocols

- CSCeh15639

Symptoms: A Cisco router may crash when it is reloaded with PIM traffic on the network.

Conditions: This symptom is observed on a Cisco 7200 series router with multicast enabled but is not platform dependent. Bootup is the most likely place where this will happen, but the router may crash anytime if an interface flap happens at the right time while receiving PIM traffic.

Workaround: There is no workaround.

- CSCei16615

Symptoms: A neighbor reloads when you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on an interface of an LSP router that functions as a tunnel headend.

Conditions: This symptom is observed when the following events occur:

- The tunnel headend sends a Path via RSVP to the neighbor but the Resv message is delayed.
- There is only one Path to the neighbor for the session.
- At the neighbor, the cleanup timer for the Path expires before the Resv message arrives, causing the session to be terminated.

Workaround: There is no workaround.

- CSCsb54823

Symptoms: One router (R2) may begin sending updates to another router (R1) before R2 has received the BGP prefix list from R1.

R1 does apply its inbound BGP prefix list so routes are denied if they need to be. However, R2 sends routes to R1 which are denied by R1.

Conditions: This symptom is observed when both routers have negotiated a BGP outbound route filter (ORF) and when R1 sends its BGP prefix list to R2.

Workaround: There is no workaround.

- CSCsb74708

Symptoms: An OSPF sham link may not form an adjacency.

Conditions: This symptom is observed when there is an interface in the global route table that has an IP address that matches the IP address of the OSPF sham link neighbor.

Workaround: Reconfigure the routers so that the IP address of the OSPF sham link neighbor does not match any IP addresses of interfaces in the global route table.

Alternate Workaround: Shut down the interface or change the IP address of the interface in the global route table.

ISO CLNS

- CSCei58655

Symptoms: A route that fails remains in the routing table with its old metric, preventing an alternate route from being used and causing a routing loop.

Conditions: This symptom is observed in a network that is configured for IS-IS and iSPF when the IP routes that are advertised in an LSP (irrespective of whether or not the LSP is fragmented) do not age-out during a rerouting failure.

Workaround: Remove iSPF from the IS-IS process by entering the **router isis** command followed by the **no ispf** command.

Miscellaneous

- CSCdz83100

Symptoms: High CPU use may occur at the interrupt level on an ingress port adapter or line card that is configured for hardware multicast when there is a high multicast traffic rate.

Conditions: This symptom is observed when policy-based routing (PBR) matches the multicast traffic and when a switchover to another interface occurs.

Workaround: Change the deny statement in the PBR configuration so traffic for multicast destination addresses is denied earlier.

Alternate Workaround: For a short while, remove the PBR configuration from the ingress interface to enable multicast traffic hardware forwarding to be established.

Further Problem Description: PBR should not influence multicast traffic and it does not when traffic is switched in the hardware. When a switchover to a new interface occurs, multicast packets are initially forwarded in the software until hardware forwarding can take over. PBR interferes with the initial software-switched packets and prevents hardware entries from being created.

- CSCef95861

Symptoms: IPv6 packets may be incorrectly forwarded by a Cisco 10720 or packet forwarding performance may be degraded significantly. Traceroute packets may be misrouted or high CPU use may occur when IPv6 packets are punted to the Route Processor.

Conditions: These symptoms are observed on a Cisco 10720 that runs Cisco IOS Release 12.0(27)S1.

Workaround: There is no workaround.

- CSCeg12134

Symptoms: When you send multicast traffic over an IPSec tunnel, a memory leak may occur on a router.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3T when both IP CEF and hardware encryption are configured. The symptom may also occur in other releases.

Workaround: Switch to software encryption for a while and then switch back to hardware encryption.

Alternate Workaround: Disable IP CEF.

- CSCeh58983

Symptoms: When a router is reloaded with a scaled L2VPN configuration, the secondary RP may reload unexpectedly because of a “BFRP HA Chkpt send” failure.

Conditions: This symptom is observed on a Cisco 12000 series that runs the c12kprp-p-mz image of a Cisco IOS interim release for Release 12.0(31)S.

Workaround: There is no workaround.

- CSCeh61467

This caveat consists of the two symptoms, two conditions, and two workarounds:

Symptom 1: After you have disabled MVPN on a VRF interface, the CPU use for the PIM process increases to 99 or 100 percent and remains at that level.

Condition 1: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB, Release 12.2SX, or a release that is based on these releases.

Workaround 1: Before you disable MVPN on the VRF interface, enable and then disable multicast routing by entering the **ip multicast-routing vrf vrf-name** global configuration command followed by the **no ip multicast-routing vrf vrf-name** global configuration command.

Symptom 2: A router that functions under stress and that is configured with a VRF interface may crash when an MDT group is removed from a remote PE router.

Condition 2: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB, Release 12.2SX, or a release that is based on these releases, and occurs only when there are frequent link flaps or other multicast topology changes that affect the VRF interface.

Workaround 2: There is no workaround.

- CSCeh97671

Symptoms: When an RP switchover occurs, the standby RP crashes, causing the switchover downtime to be longer than expected and traffic to be affected.

Conditions: This symptom is observed on a Cisco 12000 series that is configured for HA when you perform an RP switchover, when the active RP runs Cisco IOS Release 12.0(28)S4, and when the standby RP runs a Cisco IOS interim release later than Release 12.0(31)S.

Workaround: There is no workaround.

- CSCei07381

Symptoms: On a 4-port OC-48 POS Engine 4+ line card, a standard or extended access list does not deny IP packets when another link on the same line card is configured for MPLS LDP and when the router is configured for MPLS Explicit Null label support.

Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of Cisco IOS Release 12.0(30)S3 or Release 12.0(31)S.

Workaround: Remove the support for MPLS Explicit Null labels.

- CSCei07556

Symptoms: The PPP protocols flap on a 64K-port of an interface of a 1-port channelized OC-12/STM-4 (DS1/E1) ISE line card that is configured for CoS and that is congested.

Conditions: This symptom is observed when two Cisco 12000 series are connected back-to-back, when the routers are connected via 1-port channelized OC-12/STM-4 (DS1/E1) ISE line cards, and when you send real-time traffic.

Workaround: Change the QoS output policy to prevent traffic from being for longer than 10 seconds and enable keepalive packets to time out.

Further Problem Description: The symptom does not occur when you do not send real-time traffic.

- CSCei31560

Symptoms: On a 6CT3 line card on Cisco 12000 series routers, when multilink bundle is configured, the delay seen for traffic in priority queue is more than expected by about 12 to 14 msec.

This behavior is seen in all 12.0S IOS releases.

Conditions: Multilink protocol such as MFR or MLP and congestion can cause excess delay for priority traffic.

Workaround: There is no workaround.

- CSCei45956

Symptoms: A Cisco 12010 router always shows its power supplies as legacy, even if a new “intelligent” power supply is inserted in the chassis.

Conditions: This symptom occurs on the Cisco 12010 only.

Workaround: There is no workaround.
- CSCei48635

Symptoms: Multilink Frame Relay (MFR) interfaces that are configured on a channelized T3 SPA continue to flap.

Conditions: This symptom is observed on a Cisco 12000 series when you perform an online insertion and removal (OIR) of the 12000-SIP-400 in which the channelized T3 SPA is installed, or when the router reloads.

Workaround: Enter the **hw-module slot slot-number reload** command.
- CSCei51504

Symptoms: When you run an SNMP get or walk on the ifOperStatus object on a 1-port CHOC-12 OC-3 ISE line card, the status for the STS-1 path interface shows down although the channel is up.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S3.

Workaround: There is no workaround.
- CSCei69208

Symptoms: A Cisco router crashes by unexpected exception to CPUvector 300.

Conditions: This symptom is observed on a Cisco 12000 series router.

Workaround: There is no workaround.
- CSCei71478

Symptoms: A 4-port GE ISE line card that is configured with 30 or more VLAN subinterfaces may fail.

Conditions: This symptom is observed on a Cisco 12000 series that runs a Cisco IOS release that is later than Release 12.0(31)S. The symptom may also occur on a 5-port GE Engine 5 SPA.

Workaround: There is no workaround.
- CSCei72033

Symptoms: SPA goes out of service during configuration.

Conditions: This symptom occurs when thousands of MFR DLCIs are configured, IPC heartbeat failures are seen on LC console. SPA will be shut down (out of service).

Workaround: There is no workaround.
- CSCei87923

Symptoms: A policy on a main Ethernet interface does not properly match packets for one of its subinterfaces.

Conditions: This symptom is observed on a Cisco 12000 series Ethernet ISE line card when one of its subinterfaces is configured for Xconnect and has a layer 2 VPN configured and when the following events occur:

 - You attach a policy to the subinterface.
 - You remove the policy from the subinterface.

- You attach the policy to the main interface.

Workaround: There is no workaround.

- CSCei90536

Symptoms: mVPN packets have corrupted encapsulation headers.

Conditions: This symptom is observed on a Cisco 12000 series that has a channelized ISE ingress line card when packets are replicated to a VRF interface on the ingress line card, to a VRF interface on another line card, and to a core interface on a third line card. This symptom occurs only after some redundancy switchovers.

Workaround: Reload the line card.

- CSCei90588

Symptoms: A bad checksum error, bad LLS TV length error, or both are reported on a router that is configured for OSPF and BGP. These protocols or other configured protocols may flap during the errors, and data packets that are sent to the RP may be lost.

Conditions: These symptoms are observed on a Cisco router when the following conditions are present:

- OSPF, BGP, and other control protocols are configured with scaled routes and peers.
- Congestion occurs on the RP because of the control packets that are targeted to the RP in the router. Also, if additional traffic is sent to one of the IP addresses of the router, the packets are terminated on the RP. For example, IP ping packets that are directed towards one of the loopback addresses are terminated on the RP.

Workaround: There is no workaround.

- CSCei91101

Symptoms: Local switching traffic is dropped from the ToFab queue on an egress port of an 2-port T3/E3 serial shared port adapter (SPA) that is installed in a 2.5G ISE SPA Interface Processor (12000-SIP-400).

Conditions: This symptom is observed on a Cisco 12000 series that functions as a PE router in an L2VPN environment.

Workaround: There is no workaround.

- CSCej01743

Symptoms: Traffic drops may occur when traffic is sent over MFR or Frame Relay links.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S1 or a later release and that is configured for software forwarding.

Workaround: There is no workaround.

- CSCej09234

Symptoms: The standby RP on a Cisco 12000 series may fail to come up and crash during initialization. The primary RP may generate the following error message:

```
%MBUS-6-DEADSCDY: Standby RP in slot <x> timed out.
```

Conditions: This symptom is observed only when there is a large number of files for the standby RP on the flash disk (for example, when a 1 GB flash disk is about half full) and when the average file size is also large.

Workaround: Delete files on the flash disk.

- CSCej15682

Symptoms: When multicast traffic is being sourced from different sources, and one of the sources is removed, the **show ip mroute vrf** command for the VRFs still shows that source as active.

Conditions: This symptom is observed when a source is no longer active when using the **show ip mroute vrf** command.

Workaround: There is no workaround.
- CSCej20986

Symptoms: An Engine 4 ingress line card may enter an incorrect carving state in which it sends all packets that are larger than 608 bytes to the buffer size pool (freeq) of the wrong egress line card, causing all packets that are larger than 608 bytes to be dropped. The symptom is especially noticeable when the egress line card is an Engine 2 line card.

Conditions: This symptom is observed rarely on a Cisco 12000 series.

Workaround: Reload the Engine 4 ingress line card.
- CSCej22910

Symptoms: Multicast traffic does not reach a CE which is connected via static IGMP joins to PE.

Conditions: The DecapPE should have a Tx line card with one port toward the core and another port toward the edge. Traffic from EncapPE is toward the CE. There should be static joins at DecapPE with SSM configured.

Workaround: There is no workaround.
- CSCej24169

Symptoms: High CPU usage occurs on an Engine 6 line card that processes multicast traffic.

Conditions: This symptom is observed on a Cisco 12000 series when the Engine 6 line card is an ingress line card that processes SSM multicast traffic.

Workaround: Lower the traffic rate, configure a mode other than SSM, or replace the Engine 6 line card with an Engine 4 line card.
- CSCej25402

Symptoms: Standby RP reboots continuously on STANDBY HOT (SSO) mode.

Conditions: This symptom is observed with an E3 4xGIGE card in slot 12 of the router. In any other scenario the problem will not be seen.

Workaround: There is no workaround.
- CSCej28374

Symptoms: Tracebacks were observed when applying a service policy to a main interface if a subinterface is configured. The subinterface inherits the service policy, producing the tracebacks. There was no adverse behavior of the service policy. It worked properly but triggered tracebacks.

Conditions: The tracebacks could be observed if the configuration includes subinterfaces and if a service policy is applied to the main interface.

Workaround: Remove the service policy on the main interface and apply it to the subinterface in the configuration.
- CSCin72437

Symptoms: A port adapter in a router or FlexWan module in a switch may crash when an SSO switchover occurs on a Route Processor or Supervisor Engine.

Conditions: This symptom is observed when the port adapter or FlexWan module is configured with a QoS policy.

Workaround: There is no workaround.

- CSCsa93349

Symptoms: When SFP state is changed in a SPA-based line card, it momentarily blocks all other IPC message processing on the RP. This is due to a blocking call made and suspending the IPC message handler process.

Conditions: This problem occurs when SPA-based cards are in the system.

Workaround: There is no workaround.

- CSCsb17203

Symptoms: A Cisco 12000 series that is configured with dual PRPs, that has more than one 10G Engine 5 SPA Interface Processor (12000-SIP-600), and that has a 10-port Gigabit Ethernet (SPA-10X1GE) installed in each 12000-SIP-600 may not load one of the SPA modules after a cold boot.

Conditions: The symptom is observed only when the Cisco 12000 series is powered off and powered back on. The symptom does not occur on a Cisco 12000 series that is configured with a single PRP.

Workaround: Reload the router via a warm reload.

Further Problem Description: The symptom is related to a race condition that is only observed on the Cisco 12000 series. The symptom is more likely to occur when timing becomes an issue, for example, in a configuration with a large number of interfaces as described in the Symptoms above. However, the root cause of this race condition is platform-independent and relates to the interface IfIndex synchronization. This is the reason why the fix for this caveat is integrated in releases that do not support the Cisco 12000 series.

- CSCsb33258

Symptoms: An RP crashes during BGP convergence when MVPNs are configured.

Conditions: This symptom is observed on a Cisco router after a duplicate BGP MDT extended community message is received that specifies a different Route Descriptor (RD) for an MDT that already exists for the specified MDT source and group address.

Workaround: There is no workaround.

- CSCsb53420

Symptoms: Cell loss occurs when bursty VBR ATM traffic is sent through a Cisco 12000 series 4-port ATM OC-12 ISE line card via an L2TPv3 IP tunnel to another 4-port ATM OC-12 ISE line card on another Cisco 12000 series and when the VBR traffic is sent at rates lower than what is configured on the routers (that is, at about 50 percent of the OC-12 line rate).

Conditions: These symptoms are observed on a Cisco 12000 series that is connected back-to-back via an OC-192 or OC-48 POS link to another Cisco 12000 series.

Workaround: There is no workaround.

- CSCsb59294

Symptoms: The output is stuck on a Cisco 7200 series.

Conditions: This symptom is observed when a service policy attached to a T1 or E1 ingress interface on one of the following port adapters:

- PA-MC-2T1
- PA-MC-2E1/120

- PA-MC-4T1
- PA-MC-8T1
- PA-MC-8E1/120
- PA-MC-8TE1+

Workaround: Remove the service policy from the egress interface.

- CSCsb59555

Symptoms: An Engine 3 or Engine 4+ line card may be stuck in the “request reload” state and CEF may be disabled on the line card, although the CEF table is up, as is shown in the output of the **show cef linecard** command:

Slot	MsgSent	XDRSent	Window	LowQ	MedQ	HighQ	Flags
1	8558	719895	4966	0	0	0	up
2	8560	718293	4966	0	0	0	up
3	8609	722867	4965	0	0	0	up
4	8584	721311	4965	0	0	0	up
5	8597	724307	4965	0	0	0	up
9	8586	722060	4966	0	0	0	up
10	8579	720566	4966	0	0	0	up
11	8566	719086	4966	0	0	0	up
12	8606	725072	4966	0	0	0	up
13	8597	723572	4966	0	0	0	up
*7	1	3	24	0	0	0	disabled, rrp hold
0	4058	359354	4966	0	0	0	up

VRF Default, version 5032, 5024 routes

Slot	Version	CEF-XDR	I/Fs	State	Flags
1	5032	5016	67	Active	sync, table-up
2	5032	5016	5	Active	sync, table-up
3	5032	5016	20	Active	sync, table-up
4	5032	5016	5	Active	sync, table-up
5	5032	5016	5	Active	sync, table-up
9	5032	5016	4	Active	sync, table-up
10	5032	5016	4	Active	sync, table-up
11	5032	5016	20	Active	sync, table-up
12	5032	5016	4	Active	sync, table-up
13	5032	5016	8	Active	sync, table-up
*7	0	0	4	Active	table-disabled
0	0	0	5	Active	request reload, table-up

Conditions: This symptom is observed on a Cisco 12000 series after an RPR+ switchover has occurred.

Workaround: Enter the **clear cef linecard** command for the affected line card.

- CSCsb62041

Symptoms: A newly created channelized interface may show packet and byte counts before any traffic passes through the interface.

Conditions: This symptom is observed on a Cisco 12000 series. When a channelized interface is deleted, the interface index is released. This interface index may be re-allocated when a new channelized interface is created. The counters that are associated with the index need to be cleared when an interface is deleted so that they are properly initialized if the index is subsequently re-allocated to a new interface.

Workaround: There is no workaround. Although you can clear the interface counters via the CLI, doing so does not prevent the symptom from occurring because but there is an internal counter that is used in the Tx byte and packet counts and that may cause errors in the calculations.

- CSCsb75433

Symptoms: Distributed Multilink PPP (dMLP) packets are not switched via dCEF.

Conditions: This symptom is observed on a Cisco router that is configured with multilink bundles.

Workaround: There is no workaround.

- CSCsb78898

Symptoms: A Cisco 10720 that functions as a transit router for MPLS applications such as MPLS VPN or ATOM drops MPLS packets.

Conditions: This symptom is observed when the MPLS packets have multiple labels, when the egress interface on the Cisco 10720 has the **ip mtu bytes** command enabled, and when the MPLS packet size is greater than the value for the *bytes* argument.

Workaround: There is no workaround.

- CSCsb89512

Symptoms: When an GE Engine 5 SPA forwards multicast traffic via multiple VLANs of one GE port, the content of IPv4 multicast packets becomes corrupted.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S.

Workaround: There is no workaround.

- CSCsb93720

Symptoms: Using “no <any config CLI>” command may not get synchronized to standby RP. After switchover, the interface shows configuration still enabled.

Conditions: This symptom is observed on a Cisco 12000 series router that is running the c12kprp-p-mz/gsr-p-mz image of Cisco IOS Releases 12.0(30)S and 12.0(31)S.

Workaround: Reconfigure “no <any config CLI>” command after switchover.

- CSCsb94684

Symptoms: Packet drops on SPA card with Random packet sizes.

Conditions: This issue was observed on Cisco IOS Release 12.0(30)S1 on smartbits test when random packet size was used.

Workaround: Downgrade to Cisco IOS Release 12.0(30)S.

- CSCsb95210

Symptoms: There is no traffic or traffic forwarded to an incorrect interface based upon the DSCP value of the IP packet.

Conditions: This symptom occurs when interfaces are deleted and added back with MQC.

Workaround: There is no workaround.

- CSCsc02825

Symptoms: In Cisco IOS software that is running the Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP), the router could reload while trying to access a bad virtual address.

Conditions: This symptom may be observed when LDP is being used. It will not be observed with TDP. It may happen when LDP receives a protocol message larger than 512 bytes right after receiving several Label Mapping messages smaller than 25 bytes. This problem is likely to be accompanied by the presence of one of the following error message:

Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0xD0D0D0D

The above error message may be preceded by one of the following four error messages:

```
%ALIGN-1-FATAL: Corrupted program counter
pc=0xD0D0D0D, ra=0x61164128, sp=0x64879B98
%TDP-3-BAD_PIE: peer x.x.x.x; unknown pie type 0x11E
%TDP-3-UNEXPECTED_PIE: peer x.x.x.x unexpected pie type 0x0
%TDP-3-PTCLREAD: peer x.xx.x0, read failure
```

This problem may be seen in releases that include the fix for CSCeg74562 but do not have the fix associated with this defect.

Workaround: There is no workaround.

TCP/IP Host-Mode Services

- CSCsb51019

Symptoms: A TCP session does not time out but is stuck in the FINWAIT1 state and the following error message is generated:

```
%TCP-6-BADAUTH: No MD5 digest from x.x.x.x to y.y.y.y(179) (RST)
```

Conditions: This symptom is observed on a Cisco 12000 series that is configured for BGP and that is connected to a third-party vendor router after the BGP authentication password is changed on the Cisco 12000 series.

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.0(31)S1

Cisco IOS Release 12.0(31)S1 is a rebuild of Cisco IOS Release 12.0(31)S. The caveats listed in this section are resolved in Cisco IOS Release 12.0(31)S1 but may be open in previous Cisco IOS releases. This section describes only severity 1, severity 2, and select severity 3 caveats.

Interfaces and Bridging

- CSCef01220

Symptoms: A Versatile Interface Processors (VIP) with a PA-MC-8TE1 port adapter may report its memory size as unknown even though the VIP appears to function normally, and Distributed Multicast Fast Switching (DMFS) may fail to function properly.

Conditions: This symptom is observed on a Cisco 7500 series when any of the following conditions are present:

- The mode of the controller of the PA-MC-8TE1 port adapter is not set to T1 or E1 and you insert or remove another VIP with any port adapter via an OIR.

- Irrespective of whether or not the mode of the controller of the PA-MC-8TE1 port adapter is set to T1 or E1, you insert or remove a standby RSP via an OIR.

Workaround: Enter the **card type {t1 | e1} slot [bay]** command on the PA-MC-8TE1+ port adapter and ensure that none of the controllers on this port adapter are shut down.

- CSCin88718

Symptoms: All channels on a PA-MC-2T3+ port adaptor stop sending traffic although they continue to receive packets. All interfaces will remain in up/down state.

Conditions: Once we send greater than linerate over the port adaptor, for a little while the PA locks up and never returns to normal working state.

Workaround: Perform resurrect operation on the PA. Note: this will affect all interfaces on that PA.

- CSCsa87986

Symptoms: A router may intermittently transmit corrupt PPP packets. When you enter the **debug ppp nego** and **debug ppp errors** commands, it appears that “protocol reject” packets are received from the remote end.

Conditions: This symptom is observed on a Cisco 7500 series that has only one OC3 POS port adaptor per VIP and that is configured for PPP encapsulation.

Workaround: There is no workaround.

- CSCsb04481

Symptoms: CEF may fail and the following error message is generated:

```
Interface Serial0/0:63  changed state to down
%CT3-3-LOVEFAIL: CT3-SW-PA-0/0: failed to send T3 line state change love
letter
%AMDP2_FE-5-LATECOLL: Ethernet0/0 transmit error
```

Conditions: This symptom is observed on a Cisco 7500 series that is configured with a channelized T3 port adapter.

Workaround: There is no workaround.

IP Routing Protocols

- CSCdz84521

Symptoms: Selective Packet Discard (SPD) with an IP precedence of 6 and 7 may not function correctly. Packets may be treated as nonpriority packets. SPD is used when a queue is filling (for example, because of a flap or change) and routing traffic must be guaranteed a high priority and not dropped while the interface recovers. In this situation, routing traffic with an IP precedence of 6 and 7 is not given proper priority, and the recovery process may be delayed.

Conditions: This symptom is observed with incoming traffic on any interface of a Cisco 7200 series and may be observed on other Cisco platforms as well.

Workaround: There is no workaround.

- CSCec23167

Symptoms: During BGP scalability testing, error messages and tracebacks similar to the following ones may be logged, indicating a difficulty with TCP and buffer usage:

```
%SYS-2-MALLOCFAIL: Memory allocation of 4692 bytes failed from 0x6076F714,
align
Pool: I/O  Free: 11143248  Cause: Memory fragmentation
```

```
Alternate Pool: None   Free: 0   Cause: No Alternate pool
-Process= "Pool Manager", ipl= 0, pid= 6
-Traceback= 607FE10C 607FF1EC 6076F71C 6080C1D0 6080C400
```

```
%TCP-6-NOBUFF: TTY0, no buffer available
-Process= "BGP I/O", ipl= 0, pid= 139
-Traceback= 6098B4EC 609938C8 60993C1C 60D55CE4 60D0BEB0
```

Conditions: This symptom is observed on a Cisco router that is in the processing of building BGP sessions for about 80,000 prefixes and about 1200 BGP peers.

Workaround: There is no workaround.

- CSCeg52659

Symptoms: A Cisco 7200 series may not withdraw a BGP route from an iBGP peer.

Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.3(3) when the **clear ip bgp neighbor-address soft out** command is entered for one of the members of the peer group of which the Cisco 7200 series is a member and when some changes to the outbound policy are made to the same member of the peer group. This situation causes some prefixes to remain struck in the other members of the peer group.

The symptom is a very old behavior of the BGP peer group functionality: when one member of a peer group is cleared via either a hard reset or a soft reset and a policy change causes some of the prefixes to be withdrawn, inconsistencies may occur in the routes on the other members of the peer group.

Workaround: For peer groups and neighbors that are members of a peer group, do not enter the BGP neighbor-specific **clear ip bgp neighbor-address soft out** command or the **clear ip bgp neighbor-address** command. Rather, enter the peer group-specific **clear ip bgp peer-group-name soft out** command or the **clear ip bgp peer-group-name** command.

- CSCeh33504

Symptoms: A router terminates 102,000 VPNv4 routes but route reflectors (RRs) report only a subset of the total.

Conditions: This symptom is observed on a Cisco MGX RPM-XF that runs Cisco IOS Release 12.3(11)T4 when 204 routes are configured per VRF over 496 VPNs (one VPN has about 1000 routes). However, Cisco MGX RPM-PRs that function as RRs show that only 76245 routes are terminated on the Cisco MGX RPM-XF. The symptom is platform-independent and may also occur in other releases.

Workaround: There is no workaround.

- CSCeh35246

Symptoms: A router may crash when a subinterface on which OSPF is running is deleted.

Conditions This symptom is observed when the **mpls ldp sync** command is configured under OSPF.

Workaround: There is no workaround.

- CSCeh35659

Symptoms: When the **ip bgp fast-external-fallover permit** interface configuration command is enabled on the main interface of a 4-port Gigabit Ethernet ISE line card and on a subinterface of a connected BGP neighbor, and when you enter the **shutdown** interface configuration command on the main interface, the BGP session that is established on the subinterface remains up for about 150 to 180 seconds before the BGP hold timer causes the session to go down.

Conditions: This symptom is observed on a Cisco 12000 series in an per-interface fast external fallover configuration on a 4-port Gigabit Ethernet ISE line card. However, the symptom may also occur on other platforms that function in a BGP configuration.

Workaround: There is no workaround. Note that the **ip bgp fast-external-fallover permit** command is currently not supported on subinterfaces.

- CSCeh53906

Symptoms: A stale non-bestpath multipath remains in the RIB after the path information changes, and BGP does not consider the stale path part of the multipath.

Conditions: This symptom is observed on a Cisco router that has the **soft-reconfiguration inbound** command enabled and occurs only when the BGP Multipath Loadsharing feature is enabled for three or more paths, that is, the *number-of-paths* argument of the **maximum-paths number-of-paths** command has a value of three or more.

Workaround: Disable the **soft-reconfiguration inbound** command for the neighbor sessions for which the BGP Multipath Loadsharing feature is enabled or reduce the maximum number of paths for the BGP Multipath Loadsharing feature to two.

- CSCei06089

Symptoms: Conditional advertisement of the default route via a route map does not work when you enter the **neighbor default-originate** command.

Conditions: This symptom is observed on a Cisco router that is configured for BGP.

Workaround: Disable the route map entirely. If this is not an option, there is no workaround.

- CSCei25442

Symptoms: The Border Gateway Protocol (BGP) multicast distribution tree (MDT) subaddress family identifier (SAFI) could send faulty notifications to Protocol Independent Multicast (PIM) resulting in a corrupted PIM database.

Conditions: This symptom has been observed when the BGP MDT SAFI receives BGP MDT SAFI rd 2 style updates.

Workaround: There is no workaround.

- CSCei25454

Symptoms: Connectivity loss may occur for MVPNs.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(30)S or a later release when the MVPNs function in a mixed network that has both VPNv4 RD2 prefixes for MDT updates and IPv4 MDT subaddress family identifier (SAFI) prefixes.

Workaround: There is no workaround.

- CSCei26899

Symptoms: When you reset a BGP peer, some prefixes are missing.

Conditions: This symptom is observed on a Cisco MGX8850 RPM-XF that runs Cisco IOS Release 12.3(11)T. However, the symptom is platform-independent and may also occur in other releases.

Workaround: There is no workaround.

- CSCsa87473

Symptoms: A BGP speaker may fail to send all of its prefixes to a neighbor if the neighbor sends a refresh request to the BGP speaker at the same time that the BGP speaker is generating updates to the neighbor. This situation causes the neighbor to miss some prefixes from its BGP table.

Conditions: This symptom may occur between any pair of BGP speakers.

A common scenario is that a VPNv4 PE router is reloaded and then fails to learn all prefixes from its route reflector (RR). In this configuration, the symptom occurs when the processing of a VRF configuration causes the PE router to automatically generate a route-refresh request to the RR, while the RR is still generating updates to the PE.

Workaround: There is no workaround.

- CSCsa95973

Symptoms: After a switchover, secondary traffic loss occurs for OSPF routes.

Conditions: This symptom is observed when OSPF NSF is configured on an ABR and when a prefix can be learned via an “Area 0” link or via a link through another area (that is, there are redundant paths).

Workaround: There is no workaround.

- CSCsa98059

Symptoms: Suboptimal routing occurs in an OSPF configuration or a routing loop occurs between two border routers that redistribute BGP into OSPF.

Conditions: These symptoms are observed when at least two border routers are connected via eBGP to another autonomous system, receive the same prefix over these connections, and redistribute the prefix into OSPF. Under certain conditions, for example when the eBGP session from the preferred BGP exit point to the eBGP peer flaps, the second router in the local autonomous system becomes the preferred path and redistributes the eBGP route into OSPF. When the eBGP session with the first router comes back up, the LSA should be flushed but this does not occur. This situation may create routing problems on other OSPF routers or, when BGP has a higher administrative distance than OSPF, routing loops between both border routers.

Workaround: There is no workaround.

- CSCsb01490

Symptoms: When general Bidirectional Forwarding Detection (BFD) functionality is enabled and when Border Gateway Protocol (BGP) is configured without BFD functionality, BFD sessions may be started with the BGP neighbors. This is not proper behavior: BFD sessions should not be started when BGP is configured without BFD functionality.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(31)S.

Workaround: There is no workaround.

ISO CLNS

- CSCsb07279

Symptoms: When an IPv4 prefix list is used in a redistribution command for the IS-IS router process, a change in the prefix list is not immediately reflected in the routing tables of a router and its neighbor. The change may take up to 15 minutes to take effect.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(28)S.

Workaround: To have a change take effect immediately, enter the **no redistribute route-map** command followed by the **redistribute route-map** command for the IS-IS router process.

Miscellaneous

- CSCee04893

Symptoms: A Cisco router is not able to forward traffic to a TE tunnel.

Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.0(26)S1 or a later release and that is configured for MLP and MPLS, and that has a TE tunnel.

Workaround: There is no workaround.

- CSCee43853

Symptoms: The following tracebacks are generated when a Cisco 10000 series is reloaded or when a manual or unexpected PRE switchover occurs:

```
%FIB-2-HW_IF_INDEX_ILLEGAL: Attempt to create CEF interface for unknown if with  
illegal index: 0
```

```
-Traceback= 602FF2F0 603061EC 6040257C 60099DD4 60099F20 6009A574 604D8E88604E0040  
603C85C8 603D80CC 603D8310 6048381C 6047EEC4 6047894C 60480EF4 604810CC
```

Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.0(30)S or Release 12.0(30)S1 and occurs always when Gigabit Ethernet line cards are installed in the router. The occurrence of the symptom does not depend on any other particular configuration of the router, and the tracebacks are generated only at startup, not during normal operation.

Workaround: There is no workaround.

- CSCee93598

Symptoms: An LSP ping reports that an LSP is fine although the LSP is unable to carry MPLS payloads such as VPN traffic.

Conditions: This symptom is observed on a Cisco router when MPLS echo request packets are forwarded from untagged interfaces that are directly connected to the destination of the LSP ping and when the IP time-to-live (TTL) value for the MPLS echo request packets is set to 1.

Workaround: There is no workaround.

- CSCef02056

Symptoms: An inter-AS TE tunnel continues to resignal a path that is rejected instead of switching to a second path.

Conditions: This symptom is observed when the RSVP local policy on the ASBR rejects the path message because it does not meet the policy.

Workaround: There is no workaround.

- CSCef87449

Symptoms: When you enter the **shutdown** interface configuration command on the outgoing interface of a Traffic Engineering (TE) Label Switched Path (LSP), the Resv state should be removed immediately. However, the Resv state remains until a PathTear arrives or a timeout causes the TE LSP to be torn down.

When the TE headend is a Cisco router, the PathTear is sent very quickly and the state is removed.

This symptom is short-lived and it is very unlikely to be noticed.

Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS software image that contains the fix for caveat CSCec26563 when the router has MPLS TE tunnels enabled.

A list of the affected releases can be found at

<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCec26563>. Cisco IOS software releases not listed in the “First Fixed-in Version” field at this location are not affected.

Workaround: There is no workaround.

- CSCeg26528

Symptoms: The performance of a router may be severely degraded (at approximately 90 percent of the line rate) when large packets are processed, when the MLP bundle link flaps, and when the router does not recover the MLP sequence numbers of the packets.

Conditions: This symptom is observed on a Cisco 7500 series and Cisco 7600 series that are configured for dMLP only when large packets are processed.

Workaround: There is no workaround.

- CSCeg35670

Symptoms: Shortly after a Cisco IOS software boot loader image has been downloaded, a PRP-2 may crash and does not reload.

Conditions: This symptom is observed on a Cisco 12000 series that runs the boot loader image of Cisco IOS Release 12.0(30)S.

Workaround: There is no workaround.

- CSCeg74562

Symptoms: A router may take a very long time to establish LDP sessions with its peers and advertise its label bindings. In some cases, the LDP sessions may flap.

Conditions: This symptom may occur when a Cisco router that uses LDP for label distribution has a large number (greater than 250) of LDP neighbors and several thousand label bindings to advertise.

Workaround: The time required to establish the neighbor sessions and advertise the label bindings when TDP is used in place of LDP may be substantially less. Using TDP in place of LDP will result in an acceptable convergence behavior.

- CSCeg83164

Symptoms: A router may reload when you configure an ATM VC class.

Conditions: This symptom is observed on a Cisco 7200 series and Cisco 7500 series that are configured for MPLS but may be platform-independent.

Workaround: There is no workaround.

- CSCeh05988

Symptoms: A CSC OIR may cause a 6-port channelized T3 line card that is configured for FRoMPLS to fail.

Conditions: This symptom is observed on a Cisco 12000 series that runs a Cisco IOS interim release for Release 12.0(31)S and that has its redundancy mode set to RPR.

Workaround: There is no workaround.

- CSCeh13340

Symptoms: On a Cisco XR 12000 series hardware-based forwarding line card, the receive counters in the output of the **show mpls l2transport vc** command do not work in any images for AToM.

Conditions: This symptom is observed on all hardware-based engine line cards on a Cisco XR 12000 series that is configured for AToM and Sampled NetFlow on the core-facing line cards.

Workaround: There is no workaround.

- CSCeh14012
Symptoms: A 1-port channelized OC-12/STM-4 (DS1/E1) ISE line card on a CE router may crash when many (168) MLP interfaces are deleted and reconfigured via TFTP on a directly-connected PE router.
Conditions: This symptom is observed on a Cisco 1200 series that functions as a CE router.
Workaround: There is no workaround.
- CSCeh18195
Symptoms: Packets that flow to VPNv4 destinations may be dropped for up to one second when the next-hop router clears its IS-IS overload bit after having been rebooted.
Conditions: This symptom is observed in a MPLS-TE network with one-hop TE tunnels.
Workaround: There is no workaround.
- CSCeh20156
Symptoms: When the working link flaps with two to three second intervals on CHOC12 Internet Services Engine (ISE) line cards that are configured for automatic protection switching (APS), some T1 links may remain down.
Conditions: This symptom is observed on a Cisco 12000 series.
Workaround: Reload the line card(s).
- CSCeh31764
Symptoms: A standby PRE that runs Cisco IOS Release 12.2S may crash when the primary PRE runs Cisco IOS Release 12.0S.
Conditions: This symptom is observed on a Cisco 10000 series when the primary RP is the PRE1 and runs Cisco IOS Release 12.0S and when the standby RP is PRE2 and runs Cisco IOS Release 12.2S in preparation for an upgrade switchover procedure. Due to a major version mismatch, the RPR mode is invoked automatically.
Workaround: There is no workaround.
- CSCeh39904
Symptoms: After removing a large number of Frame Relay subinterfaces, the following log is displayed:

```
SYS-3-CPUHOG: Task ran for 38160 msec (3/2), process = MDFS LC Process, PC = 41129150
```


Conditions: This symptom is observed on a Cisco 12000 series that is configured for Multicast VPN.
Workaround: There is no workaround.
- CSCeh40882
Symptoms: On a Cisco 12000 series router with a 1xChOC12/DS1 ISE line card configured with multilink MFR protocol and a MQC policy, after a reload the QoS does not get applied to the bundle. The QoS goes to the suspend mode.
Conditions: The bundle loses its QoS policy when the router is reloaded. This problem is observed when running Cisco IOS Releases 12.0(28)S1, 12.0(30)S, and an interim release for Release 12.0(31)S.
Workaround: Remove the service-policy from the bundle and re-apply it.

- CSCeh42248

Symptoms: Some %GSRSPA-3-PORT_IF_INDEX & %EELC_QOS_RES_MGR-3-HW_IDB_INDEX_NOT_FOUND messages may be seen on Engine 5 Gigabit Ethernet (GE) Shared Port Adapters (SPAs) when MPLS traffic engineering tunnel is enabled on the interface.

Conditions: This symptom is observed on an Engine 5 GE SPA in a Cisco 12000 series router that is running Cisco IOS Release 12.0(31)S.

Workaround: There is no workaround.
- CSCeh49892

Symptoms: The following incorrect error message is generated when an invalid QOS policy is applied to an L2 ATM interface before a valid policy is applied:

Remove existing Service-policy CBR before applying new Service-policy egress

Conditions: This symptom is observed only on a Cisco router that is configured with a secondary RP and ATM L2VPNs that function in the VP mode.

Workaround: There is no workaround.
- CSCeh50638

Symptoms: A 4-port Gigabit Ethernet ISE line card may crash.

Conditions: This symptom is observed on a Cisco 12000 series that is configured for multicast traffic.

Workaround: There is no workaround.
- CSCeh54615

Symptoms: LSPs that support AToM circuits may fail to come up.

Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS software image that includes the fix for DDTS ID CSCeg74562. A list of the affected releases can be found at <http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg74562>. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

Workaround: There is no workaround.
- CSCeh56377

Symptoms: VRF RP mapping continues to toggle between the RPs of two CE routers.

Conditions: This symptom is observed when a Cisco 12000 series that functions as a PE router is located between the two CE routers.

Workaround: Reset the PIM neighbor for the CE router that has the lower IP address of the two CE routers.
- CSCeh58485

Symptoms: It may take up to 180 seconds for a Parallel eXpress Forwarding (PXF) engine to reload after a toaster crash has occurred.

Conditions: This symptom is observed on a Cisco 10000 series that has a configuration with 200 VPN routing/forwarding instances and occurs only when the PXF engines restarts because of some kind of fault. The symptom does not occur when you enter the **microcode reload pxf** command.

Workaround: There is no workaround.

- CSCeh59410

Symptoms: When traffic flows from an Engine 6 line card to a link-bundle interface (a POS interface or PortChannel interface), the Engine 6 line card cannot load-balance traffic between the physical ports that are part of the link bundle. This situation may cause traffic to be lost and may prevent the interface from being used to its full capacity.

Conditions: This symptom is observed on a Cisco 12000 series that runs a Cisco IOS interim release of Release 12.0(31)S and occurs for IP-to-IP traffic and when MPLS is globally disabled

Workaround: Enable MPLS globally (default).

- CSCeh59865

Symptoms: Multilink Frame Relay bundles on a 4-port channelized T3 to DS0 SPA (SPA-4XCT3/DS0) may go down after an RP SSO switchover.

Conditions: This symptom is observed on a Cisco 12000 series that functions in a point-to-point configuration with multilink Frame Relay.

Workaround: There is no workaround.

- CSCeh60185

Symptoms: An Engine 4 plus (E4+) line card that functions in an IP-to-tag switching scenario may generate “TX192-3-PAM_MODULE” and “%TX192-3-PAM_PIM” error messages and tracebacks or may crash.

Conditions: This symptom is observed on a Cisco 12000 series when the ingress interface is an Engine 2 line card that has an input ACL and when an external LDP flap occurs that affects the Engine 4+ line card.

Workaround: There is no workaround.

- CSCeh60368

Symptoms: On a Cisco 10000 series that is configured with 6-port channelized T3 line cards, when the primary and standby PREs are each loaded with a different Cisco IOS software release (for example, Release 12.0(28)S and Release 12.0(28)S3) and when the standby PRE boots, the standby PRE may crash or other errors may occur while the standby PRE configures the channelized T3 channels.

Conditions: This symptom is observed on a Cisco 10000 series for Cisco IOS Release 12.0(27)S, Release 12.0(28)S, Release 12.0(30)S, Release 12.0(31)S or a rebuild of these releases when the standby PRE runs a Cisco IOS software release that is either older or newer than the software release on the primary PRE and when one PRE runs a software release that includes the fix for caveat CSCsa41907 and the other PRE runs a software release that does not contain the fix for caveat CSCsa41907.

Workaround: Do not perform live software upgrades. Rather, bring the primary PRE down and boot the standby PRE with the same Cisco IOS software release that runs on the primary PRE, so that when both PREs come up, their software releases match.

Otherwise, upgrade to an image containing the fix for CSCeh60368.

Further Problem Description: When both the primary and standby PRE run a Cisco IOS software release that contains the fix for caveat CSCsa41907, the symptom does not occur.

- CSCeh64632

Symptoms: After a route processor or line card has reloaded, the queue limit that is set for the class default is not properly programmed.

Conditions: This symptom is observed on a Cisco 12000 series 1-port channelized OC-12/STM-4 (DS1/E1) ISE line card that has an egress policy applied to a serial interface.

Workaround: There is no workaround.

- CSCeh65748

Symptoms: A Engine 3 ISE line card may not properly handle incoming bad IP packets but may generate a traceback and a transient error message:

```
%GSR-3-INTPROC: Process Traceback= 400E10B4 400FBA2C
-Traceback= 4047917C 405E5274 400F4B58
%EE48-3-BM_ERRS: FrFab BM SOP error 40000
%EE48-3-BM_ERR_DECODE: FrFab SOP macsopi_bhadr_pkt_len_zero_err
```

```
%GSR-3-INTPROC: Process Traceback= 400E1090 400FBA2C
-Traceback= 4047917C 405E5274 400F4B58
%LC-4-ERRRECOVER: Corrected a transient error on line card.
```

The line card may also crash.

Conditions: These symptoms are observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(26)S1 or Release 12.0(26)S5a.

Workaround: There is no workaround.

- CSCeh66946

Symptoms: An interface stops traversing traffic through an Engine 6 2xOC192 POS line card.

Conditions: This symptom occurs when AToM is configured on an Engine 6 2xOC192 line card (facing the edge).

Workaround: There is no workaround.

- CSCeh73978

Symptoms: When configuring service policies on any interface, the console erroneously displays a message indicating that Rate Limit and Policing can only be configured together on 4 port ISE Ethernet cards. More importantly, it prevents the service policy from being applied to the interface.

Conditions: This symptom has been observed on startup or anytime the configuration is entered.

Workaround: There is no workaround.

- CSCeh78918

Symptoms: When a line card has reloaded because you reloaded the router, the line card crashed, or you entered a command to reload the line card, the following message may appear on the console:

```
%MDS-2-RP: MDFS is disabled on some line card(s). Use "show ip mds stats linecard" to view
status and "clear ip mds linecard" to reset.
```

This message may be generated because MDFS is erroneously disabled on the reloaded line card. Erroneous disabling of MDFS may unnecessarily extend network convergence time.

Conditions: This symptom is observed on a distributed router or switch such as a (Cisco Catalyst 6000 series, Cisco 7500 series, Cisco 7600 series, Cisco 10000 series, and Cisco 12000 series. The symptom occurs when the router has the **ip multicast-routing distributed** command enabled for any VRF and when a line card is reloaded more than 50 seconds into the 60-second MDFS flow-control period.

Workaround: The symptom corrects itself after 60 seconds. Alternatively, you can enter the **clear ip mds linecard slot number** command.

- CSCeh82971

Symptoms: A Cisco router crashes when performing an FPD image upgrade operation.

Conditions: This symptom can occur if the sending of the FPD image from RP to a line card fails because the target card is reloaded during this time window.

Workaround: Do not reload or physically remove the target upgrade line card when performing an FPD image upgrade.

- CSCeh84320

Symptoms: The subinterface on the modular GE/FE card stops forwarding.

Conditions: This symptom occurs whenever the operator enters sub-interface mode with an `xconnect` statement on the EPA-GE/FE-BBRD fixed port on the modular GE/FE card.

Workaround: While in the sub-interface mode, the operator can enter a **shutdown** command followed by a **no shutdown** command which allows the subinterface to resume forwarding.

Each time the operator enters the sub-interface on the fixed port, the workaround will need to be applied.

- CSCeh84740

Symptoms: An RPR+ switchover may cause a VIP or line card to pause indefinitely.

Conditions: This symptom is observed when a high load of traffic passes through interfaces of a VIP or line card when these interfaces are configured for QoS.

Workaround: There is no workaround.

- CSCeh97080

Symptoms: When Multiprotocol Label Switching (MPLS) is enabled on a router, one or more LDP sessions may be disrupted during periods of extremely high CPU use.

Conditions: This symptom is observed when the CPU use of the router temporarily increases to more than 90 percent for several tens of seconds and when one or more high-priority processes are frequently active but do not necessarily use many CPU cycles.

For example, high CPU use may occur when a peer router is reloaded or when an interface with several hundreds of numbered IP subinterfaces comes up, which causes many processing changes on the router because of the “Tagcon Addr” process.

On a Cisco 12000 series, high CPU use may occur because of the “Fabric ping” high-priority process, which is frequently active.

Other high-priority processes may also cause the symptom to occur.

Workaround: To increase the length of the hello adjacency holdtimes, enter the **mpls ldp discovery hello holdtime** command on the affected router. You may need to enter this command on all platforms in the network in order to provide full protection.

- CSCeh97281

Symptoms: On a Cisco 12000 series on an Frame Relay subinterface on a CT3 interface, Route Processor (RP) generated packets (such as OSPF hello) are not queued in the correct TX CoS queue.

Conditions: This issue can be seen on a Frame Relay subinterface on a CT3, when an egress MQC policy is applied. The egress policy has to match “IP precedence 6”. In this case any RP generated control packets with IP precedence 6 are not being enqueued to the correct class-matched queue.

Workaround: There is no workaround.

- CSCeh97760

Symptoms: In the outputs of the **show ip psa-cef** and **show ip cef** commands for an Engine 2 ingress line card, the “Local OutputQ (Unicast)” information may point to another and incorrect slot than the slot that the global CEF table points to.

When this symptom occurs, packets that are destined for these specific IP address are dropped.

Conditions: This symptom is observed on a Cisco 12000 series when an Engine 2 line card is used as an ingress line card for traffic that is directed to a default route.

Workaround: Enter the **clear ip route 0.0.0.0** or **clear ip route *** command.

- CSCeh97829

Symptoms: An RP may crash continuously when you reload all the line cards in a dual-RP router that has the redundancy mode is set to SSO.

Conditions: This symptom is observed on a Cisco 12000 series that is configured with two GRPs or two PRPs that are configured for SSO and occurs only when a 1-port channelized OC-48 ISE line card, a 4-port channelized OC-12 ISE line card, or 16-port channelized OC-3 ISE line card is present in the router.

Workaround: Set the redundancy mode to RPR or RPR+.

- CSCei00027

Symptoms: On a channelized OC-48 ISE line card with APS configured, a “Signal Failure” condition remains after the line card has been reloaded or after you enter the **shutdown** command followed by the **no shutdown** command.

Conditions: This symptom is observed on a Cisco 12000 series and affects only a channelized OC-48 ISE line card with an APS configuration.

Workaround: There is no workaround.

- CSCei03674

Symptoms: Class-default counters (that is, the total number of packets) do not increment.

Conditions: This symptom is observed on a Cisco router when a class map matches an OAM that is applied to a policy.

Workaround: There is no workaround.

- CSCei04350

Symptoms: MVPN PIM neighbors that are associated with both a 1-port channelized OC-48 ISE line card and a 1-port channelized OC-12 (DS1) ISE line card bounce when you perform a microcode-reload of a 1-port channelized OC-12 (DS1) ISE line card.

Conditions: This symptom is observed on a Cisco 12000 series.

Workaround: There is no workaround.

- CSCei04912

Symptoms: If a 4-port Engine 3 Gigabit Ethernet (GE) line card is fast reroute (FRR) headend, and only the RX cable is pulled out, convergence time is greater than 50ms.

Conditions: This symptom occurs when the 4-port Engine 3 GE line card is FRR headend, and only the RX cable is pulled out.

Workaround: There is no workaround.

- CSCei05312

Symptoms: An EERP-3-INVALID_LAYER error message may be generated followed by continuous tracebacks that flood the screen, causing some tracebacks to be dropped.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S and that is configured with an ATM VC and VP when a policy map of the following type is attached and when OAM traffic is sent on the VC or VP:

```

policy foo
  class oam
    set mpls exp 6
  class class-default
    police xyz cps conform-action transmit exceed-action drop
    service child
  policy child
    class clp0
      police abc cps conform-action transmit exceed-action drop

```

Workaround: Remove the above-mentioned policy from the VP or VC.

First Alternate Workaround: Stop sending the OAM traffic.

Second Alternate Workaround: Configure an alternative policy such as the following one:

```

policy foo
  class class-default
    police xyz
    service child
  policy child
    class oam
      set ...
    class clp
      set ...
    class class-default
      police xyz cps

```

- CSCei07805

Symptoms: When a router has a large VRF configuration and a lot of routing information, the following error messages may be generated during an SSO switchover:

```
%FIB-3-FIBDISABLE: Fatal error, slot/cpu 5/0: keepalive failure
```

The following CPUHOG error message and traceback may also be generated:

```
%SYS-3-CPUHOG: Task is running for (2000)msecs, more than (2000) msecs
```

```
(272/145),process = IPC LC Message Handler.
```

```
-Traceback= 40EAF5D8 411DBE94 411DBFB8 411DC5D0 411DEFEC 411DEE90 411E0200 41093100
410932B8
```

After the FIBDISABLE error messages has been generated, the router may no longer function properly.

Conditions: This symptom is observed on a Cisco 7600 series but is platform independent.

Workaround: There is no workaround.

- CSCei07946

Symptoms: When the active rate for a destination PE router is evenly distributed at 4 pps for 20 flows and the active rate for a destination CE router is evenly distributed at 4 pps for 19 flows, one flow is reported at twice that rate (that is, 8 pps).

Conditions: This symptom is observed on a Cisco 12000 series that functions in a MVPN VRF-Lite environment with 20 multicast streams that have a single sustained cell rate (SCR) and that have the pps rate evenly distributed across all streams.

Workaround: There is no workaround.

- CSCei08381
Symptoms: Engine 3 and Engine 5 line cards in a Cisco 12000 series may fail continuously.
Conditions: This symptom is observed on a Cisco 12000 series that runs a Cisco IOS interim release for Release 12.0(32)S when control-plane policing is configured on the line cards in the router.
Workaround: There is no workaround.
- CSCei08472
Symptoms: The following error message is displayed:

```
tb2-pe22(config)#pol p1
tb2-pe22(config-pmap)#class match_prec1
tb2-pe22(config-pmap-c)#band per 2
Service-policy is not supported on interface Multilink100.
```


Conditions: This symptom occurs when a service policy that is attached to a multilink interface with no members is modified.
Workaround: There is no workaround.
- CSCei08823
Symptoms: When a ToFab FCRAM single-bit error (SBE) occurs on an Engine 5 line card, the following error message is generated, and the line card resets:

```
Tofab BMA has lost a command
```


Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S and occurs only on an Engine 5 line card.
Workaround: There is no workaround.
- CSCei09755
Symptoms: When you remove a multilink bundle by entering the **no ppp multilink** command under a serial link configuration, a serial link that is configured in the multilink bundle remains in the “line protocol down” state and does not recover.
Conditions: This symptom is observed on a Cisco 7600 series that is configured with a SIP1 line card in which a SPA-CT3 is installed and on a Cisco 12000 series that is configured with a SIP-400 or SIP-600 in which a SPA-CT3 is installed.
Workaround: Reload the SPA by entering the **hw-module subslot slot subslot reload** command.
- CSCei12538
Symptoms: Using the **show ssm id** command on a line card after a switchover may crash the line card.
Conditions: This symptom is observed in Cisco IOS Release 12.0(31)S on dual RP platforms that are running high availability (HA). After a switchover, if the **show ssm id** command is issued on a line card, the line card may crash.
Workaround: Do not use the **show ssm id** on a line card.
- CSCei12771
Symptoms: All traffic with a 0 label plus another label is dropped by a 3-port Gigabit Ethernet egress ISE line card.
Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S.
Workaround: There is no workaround.

- CSCei15701

Symptoms: The active PRP pauses indefinitely after it changes from standby to active.

Conditions: This symptom is observed when the redundant PRPs are configured for RPR+ mode, the router has two APS-protected CHOC12 line cards, the router has mVPNs configured, and the router runs Cisco IOS Release 12.0(28)S3.

Workaround: There is no workaround.

- CSCei18287

Symptoms: When there are some incomplete xconnect configurations or rapid succession of unprovisioning and provisioning of xconnect, memory leaks may be observed on line cards in Segment Switch Manager (SSM).

Conditions: This symptom occurs in Cisco IOS Release 12.0(31)S or later releases.

Workaround: There is no work around.

- CSCei22697

Symptoms: Some MVPN tunnels are mapped to an incorrect VRF forwarding table.

Conditions: This symptom is observed on a Cisco router that is configured for data MDT groups.

Workaround: There is no workaround.

- CSCei27448

Symptoms: A router may crash while displaying the output of the **show ip pim mdt bgp** command.

Conditions: This symptom is observed when withdraws for a MDT source group are received by PIM from BGP while you enter the **show ip pim mdt bgp** command.

Workaround: There is no workaround. To reduce the chance of the router crashing, change the *screen-length* argument in the **terminal length screen-length** command to 0. Doing so prevents the router from pausing between multiple output screens. (The default of the *screen-length* argument is 24.)

- CSCei29398

Symptoms: A standby RP crashes when you add or remove classes from a QoS policy or when a policy is applied to one line rather than to multiple lines.

Conditions: This symptom is observed on a Cisco 12000 series but is platform-independent.

Workaround: There is no workaround.

- CSCei32294

Symptoms: An Engine 5 line card crashes.

Conditions: This symptom occurs when an OC192 SPA was inserted into the Engine 5 line card.

Workaround: There is no workaround.

- CSCei35132

Symptoms: A Cisco 12000 series router that is running Cisco IOS Release 12.0 (31)S and an Engine 3 4xOC3 line card. The topology looks like the following:

PE ----- P --- oc3 --- P ----- PE

1-hop primary tunnels are between every pair of routers above. Every link is protected by a NHOP backup tunnel LSP.

When pulling TX fiber from an Engine 3 4xOC3 line card (P2-P3 link), we occasionally see 100% packet loss in ATOM and L3VPN traffic that was going through P-P link as the primary path.

One P shows “Untagged” entries in its LFIB, especially for one PE loopback. This breaks forwarding for all the L2/L3 VPNs hanging off that PE.

The issue is timing dependent. It does not happen all the time and does not seem to be Cisco 12000 series line card dependent.

Conditions: This symptom occurs when pulling TX fiber on a POS link between two Cisco 12000 series routers.

Workaround: There is no workaround.

Further Problem Description: One of the symptoms that becomes apparent is that Primary Tunnel LSP goes down between the two Ps, and so is directed LDP session within the tunnel. This makes VPN prefixes protected by Backup TE LSP entries in the LFIB “Untagged” because LDP goes down.

- CSCei36381

Symptoms: When QOS parameters are changed, traffic does not pass via an L2TPv3 link.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S when QOS or HQoS parameters are changed and affect the traffic flow.

Workaround: Reload the affected line card or reload the router.

- CSCei37227

Symptoms: You cannot link a CoS slot table definition to a line card by entering the **rx-cos-slot** global configuration command. When you attempt to do so, the following error message is generated:

```
% Unknown Cos Queue Group - ToFab-Policy
```

Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of a Cisco IOS interim release later than Release 12.0(31)S.

Workaround: There is no workaround.

- CSCei37523

Symptoms: When you reload all the line cards on a Cisco 12000 series or when you initiate an RP switchover, a %PRP-3-CHP_DESCQ_FULL error message may be generated and some of the line cards may fail.

Conditions: This symptom is observed on a Cisco 12000 series that runs a Cisco IOS interim release later than Release 12.0(31)S when one of the clock and scheduler cards (CSCs) is shut down.

Workaround: Reload the affected line cards.

- CSCei38116

Symptoms: ISE line cards crash when a Cisco 12000 series receives 640,000 multicast streams.

Conditions: This symptom is observed when the memory of the ISE line cards becomes exhausted when the thousands of multicast streams are received.

Workaround: There is no workaround.

- CSCei39383

Symptoms: Interface configuration parameters are not applied to the running configuration after an RPR+ switchover.

Conditions: This symptom is observed intermittently on a Cisco 12000 series that is configured with a 1-port CHOC-48 ISE line card but may also occur with other line cards.

Workaround: Apply the configuration manually to the affected interface.

- CSCei40168

Symptoms: An ATOM VC that is configured on a Fast Ethernet or Gigabit Ethernet interface may not be functional and packets that are received on the interface are dropped.

Conditions: This symptom is observed on a Cisco 10720.

Workaround: Reconfigure the **xconnect** command on the affected interface.

Further Problem Description: When the symptom occurs, the output of the **show hardware pxf cpu statistics interface interface-name detail** command shows that the packets that are received on the interface are dropped because of an “mpls undefined port” condition.

- CSCei40506

Symptoms: Performance drops to 90 percent when the “N flag” is set incorrectly for the MDFS process.

Conditions: This symptom is observed on a Cisco 12000 series that is configured for mVPN, that uses an Engine 3 line card for imposition, and that uses an Engine 4+ line card for disposition.

Workaround: Reload the router.

- CSCei40645

Symptoms: When a Gigabit Ethernet (GE) link goes down between two 4-port GE ISE line cards, the link detection mechanism is inconsistent.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S.

Workaround: There is no workaround.

- CSCei48728

Symptoms: New subinterfaces and duplicate IP addresses are unexpectedly created for member interfaces of a port-channel subinterface.

Conditions: This symptom is observed on a Cisco 12000 series that is configured with dual Route Processors that function in RPR mode when a clock and scheduler card (CSC) is shut down before an RPR switchover occurs.

Workaround: There is no workaround.

- CSCei48972

Symptoms: After a manual switchover occurs in RPR+ mode, a VPN that is configured on a Frame Relay subinterface fails to recover and CEF may be disabled on line cards.

Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of a Cisco IOS interim release for Release 12.0(30)S2.

Workaround: Enter the **hw-module slot slot-number reload** command.

- CSCei49180

Symptoms: A standby RP resets when you add a channel group by entering the **channelized [mode t1 | e1]** command on the controller of a T3 port that had the **no-channelized** command enabled before you made the change.

Conditions: This symptom is observed on a Cisco 12000 series that has two RPs and that is configured with a 4-port channelized T3 to DS0 Shared Port Adapter (SPA) that is installed in a 2.5G ISE SPA Interface Processor (SIP).

Workaround: There is no workaround.

- CSCei52380

Symptoms: The entry for a tunnel is missing from the mplsOutSegmentTopLabel column of the MPLS-LSR-MIB.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4 when a mibwalk is performed on the mplsOutSegmentTopLabel object.

Workaround: There is no workaround.

- CSCei58551

Symptoms: A 1-port OC-192 Engine 4+ line card (OC192E/POS) or a Modular GbE Engine 4+ line card (EPA-GE/FE-BBRD with EPA-3GE-SX/LH-LC) may crash when an SSO switchover occurs or when the router reloads.

Conditions: This symptom is observed on a Cisco 12000 series that runs a c12kprp-p-mz image of Cisco IOS Release 12.0(31)S and that has two RPs.

Workaround: There is no workaround.

- CSCei61732

Cisco IOS may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.

Cisco has made free software available that includes the additional integrity checks for affected customers.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml>.

- CSCei64939

Symptoms: When a service policy is attached to an ATM PVP as an output policy that contains a queue limit, the policy is rejected with the error message “No ATM VC associated with this service policy.”

Conditions: This symptom is observed only for ATM VP connections when a policy is attached as an output policy with a queue limit.

Workaround: There is no workaround.

- CSCei75742

Symptoms: MPLS may fail on a router when you reload a Gigabit Ethernet (GE) line card on which Link Bundling is enabled.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S or an interim release for Release 12.0(32)S.

Workaround: Re-enable MPLS by entering the **mpls ip** global configuration command.

- CSCei75919

Symptoms: High CPU use may occur on line cards and may cause instability in control plane protocols.

Conditions: This symptom is observed on a Cisco 12000 series that functions in a mVPN decapsulation environment with core-facing Engine 4+ line cards and ISE line cards that are configured with VRFs and for hardware forwarding.

Workaround: There is no workaround.

- CSCei83644

Symptoms: A nondefault configuration becomes lost for a serial interface on a channelized OC-48 ISE line card or on a 4-port OC-12 ISE line card.

Conditions: This symptom is observed on a Cisco 12000 series after you have reloaded the router.

Workaround: There is no workaround.

- CSCei88040

Symptoms: A Cisco 12000 Engine 3 line card might be affected by a memory leak in the “CEF LC IPC Backg” process that is caused by IPv6 route changes.

If all the line card route memory is consumed, the following error messages might be seen:

```
SLOT 6:*Aug 20 07:41:23.122: %SYS-2-MALLOCFAIL: Memory allocation of 65556
bytes failed
```

```
from 0x400DCE94, alignment 32
```

```
Pool: Processor Free: 533440 Cause: Memory fragmentation
```

```
Alternate Pool: None Free: 0 Cause: No Alternate pool
```

```
-Process= "CEF LC IPC Background", ipl= 0, pid= 71
```

```
-Traceback= 40030CBC 400E22FC 400E6A38 400DCE9C 404ADB0C 404ADD80 4042354C
40425464 4114
```

```
4B08 411444AC 411443A4 4114B68C 410ECB6C 410ECEB4 410EDC3C
```

```
SLOT 6:*Aug 20 07:41:23.122: %EE48-3-IPV6_TCAM_CAPACITY_EXCEEDED: IPv6 pkts
will be soft
```

```
ware switched.
```

To support more IPv6 routes in hardware:

Get current TCAM usage with: show controllers ISE <slot> tcam

In config mode, reallocate TCAM regions e.g. reallocate Netflow TCAM to IPv6

```
hw-module slot <num> tcam carve rx_ipv6_1 <prefix> <v6-
```

```
percent>
```

```
hw-module slot <num> tcam carve rx_top_nf <nf-percent>
```

Verify with show command that sum of all TCAM regions = 100%

Reload the linecard for the new TCAM carve config to take effect

WARNING: Recarve may affect other input features(ACL,CAR,MQC,Netflow)

Doing the recarve, as suggested, will not fix the problem, except that by reloading the line card, the leaked memory will be recovered temporarily.

Conditions: This symptom occurs when continuous IPv6 routes change on an Engine 3 line card.

Workarounds:

[1] Reloading the line card can fix the problem temporarily.

[2] Disabling TCAM IPv6 lookups by emptying the IPv6 TCAM:

```
hw-module slot <slot number> tcam carve RX_IPv6_144b_REGION 128 0
```

```
hw-module slot <slot number> tcam carve RX_TOP_NF_REGION 39
```

```
microcode reload <slot number>
```

To disable [2], just use the “no” form of the command to get back to the default setting:

```
no hw-module slot <slot number> tcam carve RX_IPv6_144b_REGION 128 0
```

```
no hw-module slot <slot number> tcam carve RX_TOP_NF_REGION 39
```

```
microcode reload <slot number>
```

The default is 35% for Netflow (RX_TOP_NF_REGION) and 4% for IPv6 (RX_IPv6_144b_REGION 128).

You can check the current status of the TCAM allocation with:

```
exec slot <slot number> sh controllers tofab alpha tcam carve | i
IPv6_128|Total|Mask|RX_TOP_NF
```

Beware: With this workaround, all IPv6 packets will be process-switched on the line card, so make sure you do not have too much IPv6 traffic, or you will get 100% CPU usage on the line card and probably other problems.

[3] Enable IPv6 BGP Dampening to limit the memory leak:

```
router bgp XXX
...
address-family ipv6
bgp dampening
...
exit-address-family
```

Note: The problem was not present in Cisco IOS Release 12.0(30)S.

- CSCei90530

Symptoms: An interface of a clear channel T3/E3 SPA that is installed in a 12000-SIP-400 is in a down state after you have entered the **redundancy force-switchover** command.

Conditions: This symptom is observed on a Cisco 12000 series that is configured with two PRPs that function in RPR+ mode.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface to bring the interface back up.

- CSCsa43329

Symptoms: A Cisco 12000 series may crash because of a bus error when you configure a loopback on one of the E3 interfaces on a 6-port E3 (6E3-SMB) or 12-port E3 (12E3-SMB) line card.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S.

Workaround: Do not configure a loopback on one of the E3 interfaces.

- CSCsa57562

Symptoms: IPC messages may be generated on a 1-port channelized OC-12 (DS3) line card and the line card may be disabled and reload.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S or Release 12.0(28)SW1 when OC-3 subinterfaces are configured on the 1-port channelized OC-12 (DS3) line card, when these OC-3 subinterfaces are configured for Frame Relay, when the **rate-limit** command is enabled, and when L2TPv3 traffic is being processed.

Workaround: There is no workaround because the **rate-limit** command is not supported in a configuration in which L2TPv3 traffic is being processed.

- CSCsa59109

Symptoms: At random, subinterfaces lose the ability to ping a directly-connected peer.

Conditions: This symptom is observed on a Cisco 12000 series that is configured with two 3-port Gigabit Ethernet line cards.

Note that although regular and extended pings do not work, pings that use the record option do work.

Workaround: Reload microcode onto the affected line cards.

- CSCsa59829

Symptoms: With traffic passing over a network only occasionally, a 4-port OC12 ATM ISE line card generates a “%PM622-3-CPK24_INTR: Egr SAR timeout” error message and resets.

Conditions: This symptom is observed on a Cisco 12000 series.

Workaround: Reload the line card.

Further Problem Description: The symptom occurs when the “CPK24 FPGA” detects that the SAR does not respond in the “Utopia interface.” The SAR then crashes because of a bad canonical header in the egress direction.

- CSCsa60026

Symptoms: Cells loss occurs on a single ATM link of PA-A3-8T1IMA or PA-A3-8E1IMA port adapter.

Condition: This symptom is observed on a Cisco 7500 and 7200 series when one of the T1 or E1 member interfaces of an IMA group that is configured on a PA-A3-8T1IMA or PA-A3-8E1IMA port adapter is disconnected or when you enter the **shutdown** command on one of these T1 or E1 member interfaces. The symptom is not platform-specific and may also occur in other releases.

Workaround: There is no workaround.

- CSCsa64476

Symptoms: A Cisco 10000 series generates the following error message:

```
%GENERAL-3-EREVENT: ACLs could not add IDB to list
```

The message is followed by a traceback.

This may indicate that the standby PRE does not apply the ACL for security purposes.

Conditions: This symptom is observed on a Cisco 10000 series that is configured with redundant PREs. The symptom is a timing issue.

Workaround: There is no workaround.

- CSCsa67488

Symptoms: A Cisco 10008 router with PRE1 may report a PXF crash.

Conditions: The symptom is observed when modifying an access-list that is already attached to a multilink interface.

Workaround: Modify an access-list only if it not attached to the interface. If the access-list cannot be removed from the interface, then create a new one and apply.

- CSCsa74044

Symptoms: An RP crashes during large interface configuration changes when interfaces and QoS policies are added or deleted.

Conditions: This symptom is observed on a Cisco 12000 series when the configuration changes involve ATM and serial interfaces.

Workaround: There is no workaround.

- CSCsa77105

Symptoms: An LSP ping (or traceroute packet) is incorrectly sent from an unlabeled interface, preventing the LSP ping to detect LSP breakages when a one-hop label switched path is pinged.

Conditions: This symptom is observed on a Cisco router that is configured for MPLS OAM.

Workaround: There is no workaround.

- CSCsa77411

Symptoms: When a bandwidth change occurs, a router may crash because of a difficulty with traffic engineering link management.

Conditions: This symptom is observed on a Cisco router that integrates the fix for caveat CSCef16096 when the following conditions are present:

- The router is configured for OSPF and MPLS traffic engineering (TE).
- The interfaces, OSPF adjacencies, and TE tunnels are flapping.
- There are more than 300 OSPF interfaces (in any state, including administratively down) in the OSPF area that is configured for MPLS TE.

You can check the number of interfaces by entering the **show ip ospf** or **show ip ospf interface brief** command. Note that all interfaces that are covered by network statements are included in the command output, even those that are in the administratively down state.

A list of the affected releases can be found at

<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCef16096>. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

Workaround: There is no workaround.

- CSCsa80661

Symptoms: The data path on a 3-port Gigabit Ethernet Engine 2 (3GE-GBIC-SC) line card may be reset because of a corrupted packet that is found in the Tx SOP SRAM. This situation causes packet loss and the routing protocol sessions to flap.

Conditions: This symptom is observed on a Cisco 12000 series that runs a Cisco IOS software release that includes the fix for caveat CSCef06121. A list of the affected releases can be found at <http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCef06121>. Cisco IOS software releases that are listed in the “First Fixed-in Version” field at this location are affected.

Workaround: There is no workaround. The symptom causes a disruption of service, but service is restored.

Further Problem Description: When the symptom occurs, the following messages are generated in the log:

```
%RP-3-FABRIC_UNI: Unicast send timed out (1)
CORRUPT PACKET DUMP:
000005C000000000 0200000000000000 0000000101000000 00062AD9B40A0003
A09D008208004500 0000000000000000 0000000000000000 0000000000000000
0000000000000000 0000000000000000 0000000000000000 0000000000000000

%RPGE-6-AUTONEG_STATE: Interface GigabitEthernet1/0: Link OK -
autonegotiation complete
%RPGE-6-AUTONEG_STATE: Interface GigabitEthernet1/2: Link OK -
autonegotiation complete
%RPGE-6-AUTONEG_STATE: Interface GigabitEthernet1/1: Link OK -
autonegotiation complete
%LCGE-3-SOP_BAD_PACKET: Found corrupt pkts in tx-sop-sram. Data path was
reset.
```

```
%OSPF-5-ADJCHG: Process 1, Nbr 10.142.65.38 on GigabitEthernet1/0 from  
LOADING to FULL, Loading Done  
%OSPF-5-ADJCHG: Process 1, Nbr 10.142.65.44 on GigabitEthernet1/2 from  
LOADING to FULL, Loading Done
```

- CSCsa84587

Symptoms: A 6PE router crashes during an IPv6 ping to another PE router at the far side of the network.

Conditions: This symptom is observed when you enter the **no mpls ipv6 source-interface** command followed by **no interface type number** command in which the *type number* argument represents the IPv6 source interface that was configured in the **mpls ipv6 source-interface** command.

Workaround: When you want to disable the IPv6 source interface, first enter the **no interface type number** command in which the *type number* argument represents the IPv6 source interface that is configured in the **mpls ipv6 source-interface** command and then enter the **no mpls ipv6 source-interface** command.

- CSCsa86214

Symptoms: Locally-originated and transit packets that are greater than 1599 bytes in length do not leave a router. BGP and other TCP-based protocols that negotiate large MSS values may go down.

Conditions: This symptom is observed on a Cisco 10000 series that is configured with a PRE or PRE1 and that performs IP fragmentation.

Workaround: First, enter the **show hardware pxf cpu buffer** or **show pxf cpu buffers** command to verify buffer depletion. Then, perform a microcode-reload of the PXF engine.

- CSCsa87295

Symptoms: Traffic to a network core is dropped from a link-bundle interface of an Engine 3 line card.

Conditions: This symptom is observed when the network core is a Cisco 12000 series that runs Cisco IOS Release 12.0(26)S or a later release, that functions as a PE router, that is configured for MPLS VPN, and that has L3 loadbalancing enabled on an egress path through a link-bundle interface.

Workaround: There is no workaround.

Further Problem Description: The symptom occurs because there is incorrect FCR information in the Engine-3 hardware rewrites that point to the link-bundle interface.

- CSCsa88211

Symptoms: When you boot a Cisco 12000 series, some Layer 1 and CoS command are rejected with the following error messages:

```
Command "pos threshold sd-ber 9" not allowed on link-bundle member interface  
POS1/0
```

```
Command "tx-cos TEST" not allowed on link-bundle member interface POS1/0
```

Conditions: This symptom is observed on a Cisco 12000 series when a POS interface of an Engine 0 or Engine 2 line card has the **tx-cos** command enabled and is a member of a port channel or POS channel.

Workaround: There is no workaround.

- CSCsa88340

Symptoms: Unicast traffic that travels over an ATM subinterface between a PE router and a CE router stops.

Conditions: This symptom is observed on a Cisco 12000 series that functions as a PE router and that is configured with an ATM ISE line card when the following conditions are present:

- Remove the VRF that has only the ATM subinterface associated to it.
- Define a new VRF and remap the ATM subinterface to this new VRF.
- Enable RPF on the ATM subinterface.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the ATM subinterface or remove and re-add the ATM subinterface configuration.

- CSCsa93814

Symptoms: Sending high-rate Multicast and Unicast bi-directional traffic can cause the PXF complex to pause indefinitely and recover.

Conditions: This symptom has been observed when sending IP Multicast, high-rate bi-directional Unicast and Multicast traffic between 4 GE ports across an SRP uplink.

Workaround: There is no workaround.

- CSCsa96275

Symptoms: When you send traffic with the full bandwidth of an IMA bundle, cell loss occurs. For example, cell loss occurs when you send traffic with more than 5 Mbps on an 8-link T1 IMA group or with 6.4 Mbps on an 8-link E1 IMA group.

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(30)S and that is configured for ATM L2TPV3, cell-packing, and multiple VP configurations. There is no cell loss with a single PVC without an L2TPv3 configuration.

Workaround: There is no workaround.

- CSCsa96941

Symptoms: When VBR ATM traffic is sent through a Cisco 12000 series 4-port ATM OC-3 ISE line card via an L2TPv3 IP tunnel to another 4-port ATM OC-3 ISE line card on another Cisco 12000 series, the VBR ATM traffic passes at lower rates than what is configured on the routers, and cell loss occurs.

Conditions: These symptoms are observed on a Cisco 12000 series that is connected back-to-back via an OC-192 POS link to another Cisco 12000 series.

Workaround: There is no workaround.

- CSCsa97238

Symptoms: A 2.5G ISE SPA Interface Processor (SIP) in which a 4-port channelized T3 to DS0 Shared Port Adapter (SPA) is installed crashes when the controller is reconfigured and VRFs are present or have been present on the associated interfaces.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S.

Workaround: There is no workaround.

Further Problem Description: The SIP and SPA do not recover on their own; you must reload the router to recover the SIP and SPA.

- CSCsa99983

Symptoms: New ATOM or L2TPv3 sessions may not come up.

Conditions: This symptom is observed on a Cisco router that is configured for Multilink Frame Relay (MFR) over L2TPv3/AToM when there are services with incomplete MFR over L2TPv3/AToM configurations and when the router has run for a long period of time.

Workaround: There is no workaround.

- CSCsb00493

Symptoms: Packets do not switch through a core interface of a line card that has hardware acceleration enabled.

Conditions: This symptom is observed on a Cisco 12000 series when the line card that contains the core interface has also a VRF interface that is shut down.

Workaround: Disable hardware acceleration on the line card.

- CSCsb02964

Symptoms: When a class map that contains an access control list (ACL) that is too large and complex to fit in memory is applied to an MQC policy map on a Cisco 10720, the router pauses indefinitely while compiling the ACL and generates a MALLOCFAIL error. The router should report an out-of-memory situation.

Conditions: This symptom is observed when the ACL contains 2000 lines and is complex.

Workaround: There is no workaround.

- CSCsb04721

Symptoms: When the Any Transport over MPLS (AToM) feature is enabled on a router, AToM virtual circuits to a peer may not be re-established after an interface flap or after being reconfigured, because the required targeted Label Distribution Protocol (LDP) session is not re-established.

Conditions: This symptom is observed when LDP is not configured on any interfaces via the **mpls ip** interface configuration command, which is typically the case when MPLS Traffic Engineering (TE) tunnels are used to transport AToM traffic between endpoints and when the **mpls ip** interface configuration command is not enabled on any TE tunnels.

The symptom occurs in Cisco IOS software releases that include the fix for caveat CSCec69982 when any form of one of the following commands is configured on the router and appears in the running configuration:

```
- mpls ldp explicit-null
- mpls ldp advertise-labels
- mpls ldp session protection
- mpls ldp password fallback
- mpls ldp password option
- mpls ldp password required
```

A list of the affected releases can be found at

<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCec69982>.

Workaround: Enter the **mpls ip** command on a TE tunnel interface or temporarily on a physical interface to force LDP to be re-established.

- CSCsb05218

Symptoms: An IPv6 ACL configuration may be lost or incorrect after an SSO switchover.

Conditions: This symptom is observed when a Cisco 12000 series performs IPv6 ACL filtering and when the ACL is modified.

Workaround: There is no workaround.

- CSCsb06383

Symptoms: When sending high rate Multicast and Unicast bi-directional traffic back to back between 4 Gigabit Ethernet ports and across the SRP uplink interface, the PXF complex occasionally stops running. The PXF complex restarts and functionality is restored automatically.

Conditions: This symptom has been observed with high rate Multicast and Unicast traffic.

Workaround: Recovery is automatic.
- CSCsb09190

Symptoms: A router misses an entry in its label forwarding table, which is shown in the output of the **show tag-switching forwarding-table** EXEC command for the missing entry and in the output of the **show ip cef detail** EXEC command for the prefix.

Conditions: This symptom is observed on a Cisco router that is configured for Multiprotocol Label Switching (MPLS) and that learns its routes through iBGP from redundant route reflectors (RRs) when BGP labeling is not enabled.

Workaround: There is no workaround. However, when you enter the **clear ip route** EXEC command for the affected prefix, the prefix is reinstalled in the label forwarding table.
- CSCsb11574

Symptoms: After a Cisco 12000 series is rebooted, the interfaces that are associated with a 6-port channelized T3 (T1) line card may not come up.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S.

Workaround: Reload the line card to bring up the controllers and interfaces.
- CSCsb14213

Symptoms: When IPv4 multicast packets have a resultant IP checksum of “FFXX”, the checksum becomes corrupt.

Conditions: This symptom is observed on a Cisco 10720 that runs Cisco IOS Release 12.0(31)S.

Workaround: There is no workaround.
- CSCsb14703

Symptoms: The PXF engine of a Cisco 10000 series crashes.

Conditions: This symptom is observed when a Fast Ethernet port flaps because you change the duplex configuration.

Workaround: Do not change the duplex mode.
- CSCsb17153

Symptoms: A serial interface that is configured for CRC-16 will revert to CRC- 32 when a router reloads.

Conditions: This symptom occurs when configuring a serial interface on a Cisco 12000 series router that is running Cisco IOS Release 12.0(31)S and is utilizing a 4xCT3/DSO adapter in an Internet Service Engine (ISE) 2.5G SPA line card for CRC-16. When the configuration is written and the router reloads, the interface will come up as CRC-32.

Workaround: There is no workaround.
- CSCsb18880

Symptoms: A 4-port channelized STM-1/OC-3 line card resets and generates an “IRONBUS-FAULT” error message.

Conditions: This symptom is observed on a Cisco 10000 series when you enter the **tug-2** *tug-2-number e1 e1-number loopback* command on the line card.

Workaround: There is no workaround.

- CSCsb27311

Symptoms: After you have send linerate traffic via an IMA interface for a while, a ping fails in a packed cell relay configuration via ATM over L2TPv3 pseudowires.

Conditions: This symptom is observed in a scalable packed cell relay configuration on an IMA interface of a PA-A3-8E1IMA or PA-A3-8T1IMA port adapter that is installed in a Cisco 7200 series or Cisco 7500 series.

Workaround: There is no workaround.

- CSCsb29326

Symptoms: An snmpwalk for cmplsFrrFacObjects for the FRR-MIB fails to show entries for a tunnel headend.

Conditions: The symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(26)S6, Release 12.0(28)S3, or Release 12.0(31)S.

Workaround: There is no workaround.

- CSCsb34838

Symptoms: A line card or port adapter may generate SYS-6-STACKLOW error messages and reload because of a software forced crash. The crashinfo file shows that the crash is caused by the CEF Scanner process that is related to recursive calls:

```
%SYS-6-STACKLOW: Stack for process CEF Scanner running low, 0/6000
```

The output of the **show cef events** command for the line card or port adapter shows that a CPU hog condition occurs after the CEF Scanner process:

```
...
Process Scanner event loop enter
CPUHOG -1ms XDRtyp 8=control len=11 Hex:0F0000079C00FA00
CPUHOG 2044ms XDRtyp 8=control len=13 Hex:08000000038E2A541A01
Flag FIB switching running set to yes
+3d04h CPUHOG -4ms XDRtyp 69=TFIB_FRR_UNPROTECT_TRANSIT len=15
Hex:020001F40000000400000000
```

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(31)S.

Workaround: There is no workaround.

- CSCsb41367

Symptoms: When you enter the **redundancy force-switchover** command, an Engine 4 line card may crash.

Conditions: This symptom is observed on a Cisco 12000 series that runs the c12kprp-p-mz Cisco IOS software image and that has two RPs that function in SSO mode.

Workaround: There is no workaround.

- CSCsb54190

Symptoms: When you shut down an SRP interface on which the egress L2 priority is set to high by entering the **no shutdown** interface configuration command, the PXF engine of a downstream router may crash.

Conditions: This symptom is observed on a Cisco 10720.

Workaround: Do not enter the **no shutdown** interface configuration command. Rather, force a ring wrap by entering the **srp ips forced-switch** command.

Wide-Area Networking

- CSCef54653

Symptoms: Some members of a multilink bundle remain inactive, while others are active.

Conditions: This symptom is observed when the interfaces are configured with the **ppp chap hostname** or **ppp multilink endpoint** command. Very high speed interfaces may come up and join the multilink bundle faster than the configuration can be processed, which causes them to use the host name of the router (instead of the configured user name or endpoint value) as the Endpoint Discriminator during Link Control Protocol (LCP) negotiations. This situation causes a mismatch between these links and those that come up after the configuration command is processed.

Workaround: Enter the **shutdown** interface configuration command followed by **no shutdown** interface configuration command on the active links to enable the links to renegotiate LCP with the correct Endpoint Discriminator value.

- CSCeh49910

Symptoms: With automatic protection switching (APS) configuration on CHOC12 Internet Services Engine (ISE) cards, flapping the working link within a 2- to 3-second time interval may result in some of the T1 links staying down.

Conditions: This symptom has been observed with APS configuration on a CHOC12 ISE card.

Workaround: Enter a **shutdown** command and then a **no shutdown** command to clear the problem.

- CSCsa87205

Symptoms: A router that is configured for PPP Multilink reloads because of a bus error.

Conditions: This symptom is observed after a Telnet or SSH session is established when you enter the **who** command.

Workarounds: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.0(31)S

All the caveats listed in this section are resolved in Cisco IOS Release 12.0(31)S. This section describes only severity 1, severity 2, and select severity 3 caveats.

Basic System Services

- CSCed64664

Symptoms: A “%SYS-2-LINKED: Bad enqueue” error message may be seen in the syslog of an LNS right after traffic is sent through a PPP multilink bundle that is established via an L2TP session on the LNS. This message is also seen when multilink PPP fragments are switched or when multicast packets are replicated.

Certain packet buffers (particle clones) are eventually depleted, and multilink fragmentation stops working when all particle clones are exhausted. You can monitor the availability of particle clones by entering the **show buffers | begin Particle Clones: EXEC** command; the command does not produce any output if no more particle clones are available.

Conditions: This symptom is observed with all features that use particles. The symptom is not specific to VPDN, GRE, or other features that use particles.

Workaround: There is no workaround.

Further Problem Description: Different symptoms may occur with different features.

- CSCee83917

Symptoms: The RP of a Cisco router may crash when entering the **write memory** legacy command.

Conditions: This symptom is observed on a Cisco router that has the **snmp mib community-map** command enabled with a very long community string and an engineID. The symptom may also occur when the long community string is removed from the configuration. The symptom does not occur when entering the **copy running-config startup-config EXEC** command.

Workaround: A community string that is shorter than 40 characters will not cause the symptom to occur.

- CSCeg15044

Symptoms: Although there are free tty lines, you cannot make a Telnet connection and a “No Free TTYs error” message is generated.

Conditions: This symptom is observed when there are simultaneous Telnet requests.

Workaround: There is no workaround.

- CSCeg16078

Symptoms: You cannot create a VRF-aware ICMP, UDP, or jitter probe using SNMP.

Symptoms: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.0(27)S. Note that the symptom does not occur in Release 12.2(11)T.

Workaround: Use CLI commands to create a probe.

- CSCeg23428

Symptoms: After you perform an OIR of a VIP, reload microcode onto a VIP, or after a VIP crashes, an MLP or MFR interface that is shut down comes up unexpectedly.

Conditions: This symptom is observed on a Cisco 7500 series only with virtual interfaces and only the first time that you perform an OIR or reload microcode or that the VIP crashes after the router has booted up. The symptom does not occur when you perform subsequent OIRs or reload microcode again or when the VIP crashes again.

Workaround: There is no workaround.

- CSCeg41734

Symptoms: The console of a router may stop responding and the router may stop forwarding traffic.

Conditions: This symptom is observed on a Cisco 7206VXR that runs Cisco IOS Release 12.3(6b) and that is configured with an NPE-G1 when the native Gigabit Ethernet interfaces of the NPE-G1 are used. The symptom may also occur in other releases.

Workaround: There is no workaround.

- CSCeh47604

Symptoms: An OER border component does not sent passive updates for OER prefixes, preventing the prefixes from being controlled. The prefixes cycle from the default state to the hold-down state back to the default state.

Conditions: This symptom is observed when NetFlow is configured and when the mode monitor is configured to be “passive” or “both”.

Workaround: Configure the mode monitor to be “active”. The functionality of the mode monitor is limited to the “active” mode only.

- CSCin79312

Symptoms: An outage may occur when you attempt to connect via the console port to a Cisco ONS 15540, and routine messages are generated that relate to the loss of light on wave ports that are turned on. Interface alarm flaps may cause a hardware watchdog timeout, and the platform may fail to switch over to the standby CPU.

Conditions: These symptoms are observed on a Cisco ONS 15540 during normal operation when optical interfaces are not used not shut down. The symptoms may be platform-independent.

Possible Workaround: Shut down any unused interfaces.

- CSCuk51587

Symptoms: The following error message is generated when you insert a VIP into a previously empty slot of a Cisco 7500 series.

```
%COMMON_FIB-2-HW_IF_INDEX_ILLEGAL: Attempt to create CEF interface for unknown if
with illegal index: 0
```

Conditions: This symptom is observed on a Cisco 7500 series that is configured for CEF.

Workaround: There is no workaround.

Interfaces and Bridging

- CSCea29435

Symptoms: A VC that is configured on an ATM PA-A3 port adapter may stop receiving traffic.

Conditions: This symptom is observed on a Cisco 7x00 router that is configured with an ATM PA-A3 port adapter when the default MTU is changed to a higher value.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the subinterface on which the VC is configured.

- CSCeb60620

Symptoms: A Cisco Route Switch Processor (RSP) that is configured as a bridge may not pass bridged traffic, regardless of the protocols that are configured on Ethernet interfaces. This situation can lead to a loss of connectivity.

Conditions: This symptom is observed on a Cisco RSP that is running a Cisco IOS rsp-jsv-mz image.

Workaround: There is no workaround.

- CSCee55632

Symptoms: A Cisco 7500 series may leave ATM PVCs up when the ATM interface is shut down.

Conditions: This symptom is observed on a Cisco 7500 series that has a PA-A3 when the CPU utilization of the VIPs is high.

Workaround: There is no workaround.

- CSCef23253

Symptoms: When you activate a serial interface on a PA-MC-8TE1+ port adapter that is installed in a VIP, dCEF may be disabled on the slot in which the PA is installed (in this example, in slot 3) and the following error message is generated:

```
%FIB-3-FIBDISABLE: Fatal error, slot 3: IPC Failure: timeout
```

The output of the **show controller vip 3 logging** command may time out, indicating problems with IPC.

The failure may cause additional error messages or may cause the VIP to reset, affecting all port adapters that are installed in the VIP.

Conditions: This symptom is observed on a Cisco 7500 series with a faulty PA-MC-8TE1+ port adapter that is installed in a VIP.

Workaround: There is no workaround. This fix for this caveat eases the detection of a faulty port adapter (see below).

Further Problem Description: The fix for this caveat will detect and shut down a faulty port adapter so that the VIP and the other port adapters in the VIP are not affected. The error message that is added by the fix is the following:

```
%VIP2 R5K-1-MSG: slot3 PA BAD - disabling the PA in bay 1
```

This message indicates that the PA-MC-8TE1+ in bay 1 is faulty and must be replaced.

- CSCef79968

Symptoms: When an **snmpget** is executed for an interface index below .1.3.6.1.2.1.31.1.1.1.6, the router responds with the following information:

```
ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifHCInOctets.12 : VARBIND EXCEPTION: No Such Instance
```

However, an **snmpwalk** executes successfully for an interface index below .1.3.6.1.2.1.31.1.1.1.6.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(26)S3 when an **snmpget** is executed for 4GE-SFP-LC subinterfaces or for a 4GE-SFP-LC interface when there is another interface index for the same interface. The symptom may be platform-independent.

Workaround: Reload the router.

- CSCeg03185

Symptoms: A few permanent virtual circuits (PVCs) go into a stuck state causing OutPktDrops on a Cisco 7200 router.

Conditions: This symptom occurs on a Cisco 7200 router running Cisco IOS Release 12.2(26) with a PA-A3-T3 ATM interface. The symptom may also occur in other releases.

Workaround: Remove and re-apply the PVC statement.

- CSCeg73645

Symptoms: A Versatile Interface Processor 2-50 (VIP2-50) crashes because of a Cybus error with DMA receive errors.

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.1 and that is configured with a PA-2FE that is installed in a VIP2-50. The symptom may also occur in other releases.

Workaround: There is no workaround.

- CSCeh10624

Symptoms: A Cisco 7206VXR may reload unexpectedly because of a bus error.

Conditions: This symptom is observed on a Cisco 7206VXR that runs Cisco IOS Release 12.3(10a) and that is configured with an NPE-G1 and a couple of PA-MC-8TE1+ port adapters. The symptom may also occur in other releases.

Workaround: There is no workaround.

- CSCeh43864
Symptoms: The line protocol on the POS interface of a PA-POS-OC3 port adapter flaps continuously.
Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS interim Release 12.3(14.10) but may also occur in other releases.
Workaround: There is no workaround.
- CSCin79468
Symptoms: An ATM subinterface enters the up/up state regardless of whether or not a PVC is down.
Conditions: This symptom is observed on a Cisco 7500 series that is configured with a PA-A3 port adapter when the router boots up without a connecting cable. This situation causes a PVC to remain down. The PVC remains down even after you connect the cable and the ATM subinterface enters the up/up state.
Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the ATM subinterface with the PVC that is down.
- CSCin84694
Symptoms: On a Cisco 7x00 series that runs Cisco IOS Release 12.3 and that is equipped with an ATM PA-A3 port adapter, the SAR chip of the port adapter may crash or the interface may become stuck.
Conditions: This symptom is observed when there is a high-traffic load on the ATM PA-A3 port adapter and when many VCs are created, deleted, and modified continuously. The symptom may also occur in other releases.
Workaround: There is no workaround.
- CSCin86455
Symptoms: Auto-provisioning may be disabled on a Cisco 7200 series that is configured with a PA-A3 port adapter.
Conditions: This symptom is observed when a VC class that is configured for create on-demand is attached to the main ATM interface and then the create on-demand configuration is removed and re-applied to the VC class.
Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the ATM interface of the PA-A3 port adapter.
- CSCin86673
Symptoms: A VC may become stuck and stop transmitting traffic.
Conditions: This symptom is observed on a Cisco 7200 series that is configured with a PA-A3 or PA-A6 port adapter when there is a high traffic load and when the QoS class of the VC is changed.
Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface that contains the affected VC.

IP Routing Protocols

- CSCdr31946
Symptoms: A Cisco router that runs Enhanced Interior Gateway Routing Protocol (EIGRP) with the stub feature enabled may have a route that is active and not waiting for replies.
Conditions: This symptom is observed only in networks where all of the EIGRP neighbors are declared as stub.

Workaround: Remove the EIGRP stub feature or clear the IP EIGRP neighbors.

- CSCdz42920

Symptoms: A router may crash because of a bus error when you configure IP accounting.

Conditions: This symptom is observed when you enter the **clear ip accounting** EXEC command.

Workarounds: Do not enter the **clear ip accounting** or **show ip accounting** EXEC command.

- CSCea31201

Symptoms: A Cisco router may reload unexpectedly because of a bus error.

Conditions: This symptom is observed on a Cisco router that has the **ip accounting** interface configuration command enabled.

Workaround: There is no workaround. The problem is rare and typically not reproducible.

- CSCed50220

Symptoms: The RP and SP MFIB tables are not synchronized, preventing the outgoing interfaces for multicast flows from matching.

Conditions: This symptom is observed when you reload a Cisco Catalyst 6000 series or Cisco 7600 series that are configured for multicast. The symptom may be platform-independent.

Workaround: There is no workaround.

- CSCef08797

Symptoms: A router may stop redistributing static routes into BGP.

Conditions: This symptom is observed when the static routes are inserted into the BGP table with a network statement that uses a route map that is configured with the **match as-path** route-map configuration command.

The symptom occurs because the **match as-path** route-map configuration command causes a non-BGP route to be denied.

Workaround: Do not use BGP-specific match statements when you source non-BGP routes.

- CSCef11304

Symptoms: When performing a snmpwalk on OSPF-MIB that supports the ospfExtLsdbTable, a router can crash. In other instances alignment errors are observed when you enter the **show alignment** command.

Conditions: These symptoms are observed on a Cisco platform that runs Open Shortest Path First (OSPF) and supports the ospfExtLsdbTable in OSPF-MIB.

Workaround: There is no workaround.

- CSCef28184

Symptoms: Multipath routes may become stale when the nexthop is unreachable, preventing a ping between two CE router from succeeding.

Conditions: This symptom is observed in a BGP environment when a multipath route is withdrawn.

Workaround: There is no workaround.

- CSCef33035

Symptoms: A router may crash and reload and generate the following error message:

TLB (load or instruction fetch) exception, CPU signal 10, PC = 0x609EE524

Conditions: This symptom is observed on a router that runs OSPF and that is configured with incremental SPF (ISPF).

Workaround: Disable ISPF by entering the **no ispf** router configuration command.

- CSCef45830

Symptoms: A stale BGP route does not time out, which can be observed in the output of the **show ip route vrf** command.

Conditions: This symptom is observed in a BGP multipath configuration.

Workaround: Enter the **clear ip route vrf vrf-name** command.

- CSCef60452

Symptoms: A router may stop receiving multicast traffic.

Conditions: This symptom is observed rarely during convergence when a router receives a Join message on an RPF interface and when a downstream router converges faster than the first router that receives the Join message.

In this situation, the router does not populate the RPF interface into the OIL (that is, the OIL remains null) because the old SP-tree has already been pruned by the downstream router. When the RPF interface of the router changes to the new path later, it does not trigger a Join message toward the multicast source until the router receives a next periodic Join message from the downstream router and populates the OIL. As a result, multicast traffic stops temporarily but no longer than the periodic Join message interval.

Workaround: There is no workaround.

- CSCef65500

Symptoms: A Cisco router that is configured for OSPF may generate recurring SYS-3-CPUHOG messages and tracebacks that are caused by the OSPF process:

```
%OSPF-5-ADJCHG: Process 100, Nbr 10.52.0.186 on ATM1/0.381 from LOADING to FULL,
Loading Done
%SYS-3-CPUHOG: Task ran for 4568 msec (243/31), process = OSPF Router, PC = 60B9DFA8.
-Traceback= 60B9DFB0 60B7E6E0 60B7EE58
%OSPF-5-ADJCHG: Process 100, Nbr 10.53.0.66 on ATM1/0.115 from FULL to DOWN, Neighbor
Down: Dead timer expired
%OSPF-5-ADJCHG: Process 100, Nbr 10.53.0.66 on ATM1/0.115 from LOADING to FULL,
Loading Done
%SYS-3-CPUHOG: Task ran for 4988 msec (569/120), process = OSPF Router, PC = 60B9DFA8.
-Traceback= 60B9DFB0 60B7E6E0 60B7EE58
```

At another date, the following error messages and tracebacks are generated:

```
%SYS-3-CPUHOG: Task ran for 2224 msec (368/9), process = OSPF Router, PC = 60BA80BC.
-Traceback= 60BA80C4 60B8876C 60B88EE4
%OSPF-5-ADJCHG: Process 100, Nbr 10.61.0.26 on ATM2/0.179 from FULL to DOWN, Neighbor
Down: Dead timer expired
%OSPF-5-ADJCHG: Process 100, Nbr 10.61.0.26 on ATM2/0.179 from INIT to DOWN, Neighbor
Down: Interface down or detached
%OSPF-5-ADJCHG: Process 100, Nbr 10.61.0.26 on ATM2/0.179 from LOADING to FULL,
Loading Done
%SYS-3-CPUHOG: Task ran for 2028 msec (647/283), process = OSPF Router, PC = 60BA80BC.
-Traceback= 60BA80C4 60B8876C 60B88EE4
%SYS-3-CPUHOG: Task ran for 2904 msec (552/153), process = OSPF Router, PC = 60BA80BC.
-Traceback= 60BA80C4 60B8876C 60B88EE4
```

Conditions: This symptom is observed on a Cisco 7200 series that is configured with an NPE-225 and that runs Cisco IOS Release 12.2(15)T5 or 12.2(15)T13. However, the symptom may be platform-independent and could also occur in other releases.

Workaround: There is no workaround.

- CSCef81489

Symptoms: If an ASBR receives a withdraw message, it does not send the withdraw message to any peer, preventing an alternate route from functioning.

Conditions: This symptom is observed when MPLS VPN inter-AS is configured.

Workaround: There is no workaround. To recover from the symptom, enter the **clear ip bgp *** command on the ASBR.

- CSCef84062

Symptoms: A Cisco router that runs BGP may crash because of a bus error at a low address when you enter the **show bgp ipv6 network** command.

Conditions: This symptom is observed on a Cisco 7505 router that runs Cisco IOS 12.2(15)T8 after BGP configuration changes. The symptom may also occur in other releases.

Workaround: There is no workaround.

- CSCef91275

Symptoms: An MPLS TE tunnel stays stuck in the “Path Half Admitting” state, as is shown by the output of the **show mpls traffic-eng tunnel** command, thereby preventing the tunnel from coming up.

Conditions: This symptom may be observed when a particular third-party router that functions as the headend for the MPLS TE tunnel sends a Path message to a Cisco router that functions as the midpoint for the router MPLS TE tunnel and that does not have the **mpls traffic-eng tunnels** interface configuration command enabled on the outbound interface that would be used to forward the Path message.

Workaround: Enter the **mpls traffic-eng tunnels** interface configuration command on the outbound interface of the Cisco router. Then, enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on this interface, and save the configuration.

- CSCef92863

Symptoms: A Cisco 10000 PRE-1 may reload when a VRF that is configured with eight maximum paths is modified.

Conditions: This symptom is observed when a VRF on the Cisco 10000 series is configured for eight maximum EIBGP paths by entering the **maximum-paths eibgp 8** command and when the VRF is modified in such a way that there is a change in the number of paths that are available. The symptom may also occur on a Cisco 10720.

Workaround: A Cisco 10000 series can support only six maximum paths. Therefore, configure the number of maximum paths by entering the **maximum-paths eibgp 6** command.

- CSCef93215

Symptoms: A router that is configured for OSPF may reload unexpectedly and reference the “ospf_build_one_paced_update” process.

Conditions: This is observed on a Cisco router that has a mixture of LSAs (of type 5 and 11) that travel throughout an autonomous system and LSAs (of any type other than type 5 and 11) that travel within a particular OSPF area. The symptom may occur at any time without any specific changes or configuration and is not specifically related to any type of LSA.

Workaround: There is no workaround.

Further Problem Description: The symptom is very unlikely to occur. The symptom does not occur on a router that has exclusively stub areas and NSSA areas. The symptom may occur when a router does not have exclusively stub areas and NSSA areas.

- CSCef95026

Symptoms: When interfaces flap, a Cisco router may reload unexpectedly because of a bus error.

Conditions: This symptom is observed when OSPF accesses a freed LSDB entry.

Workaround: There is no workaround.

- CSCef97738

Symptoms: BGP may pass an incorrect loopback address to a multicast distribution tree (MDT) component for use as the source of an MDT tunnel.

Conditions: This symptom is observed when you reload a Cisco router that runs Cisco IOS Release 12.0(28)S1 and when there is more than one source address that is used in BGP, such as Lo0 for IPv4 and Lo10 for VPN. If the IPv4 peer is the last entry in the configuration, the MDT tunnel interface uses lo0 as the source address instead of lo10. The symptom may also occur in other releases.

Workaround: Remove and add the MDT statement in the VRF.

- CSCeg07725

Symptoms: A router may continue to redistribute an eBGP route into EIGRP after the eBGP route is deleted or EIGRP may not redistribute an eBGP route after the eBGP route has been installed.

Conditions: This symptom is observed on a Cisco router that redistributes eBGP routes into EIGRP when the router functions in a multihoming environment.

The symptom occurs in a configuration with two PE routers that advertise routes via eBGP and a border router that is configured with a higher local preference than the PE routers when the eBGP route of the primary path is withdrawn and the route of the secondary path is installed.

Workaround: If a route is still redistributed into EIGRP after the eBGP route is deleted, clear the BGP peer from which the eBGP route used to be learned so EIGRP stops advertising the route.

If a route is not redistributed into EIGRP after an eBGP route is installed, clear the route so EIGRP starts advertising it. Another workaround is to enter the **bgp redistribute-internal** command to cause EIGRP to redistribute iBGP routes and to prevent EIGRP from failing to redistribute an updated BGP route.

- CSCeg31951

Symptoms: A router that is configured for BGP may send incorrect or incomplete updates to its neighbors.

Conditions: This symptom is observed on a router that has the **neighbor remove-private-as** and **neighbor as-override** command enabled.

Workaround: There is no workaround.

- CSCeg35811

Symptoms: A platform (that is, a switch or a router) may crash when you enter the **ip routing** command followed by the **configure memory** command and the **no ip routing** command multiple times. Multiple tracebacks may also be generated.

Conditions: The symptom is observed on a Cisco platform that functions as the master in a stacked environment and that is configured for OSPF. The symptom is more likely to occur when the platform functions under a heavy traffic load.

Workaround: Do not enter the **ip routing** command followed by the **configure memory** command and the **no ip routing** command multiple times.

- CSCeg49796

Symptoms: Commands on a router may be unexpectedly removed from the running configuration.

Conditions: This symptom is observed on a router that is assigned as a neighbor to a BGP peer group. For example, when the **shutdown** command was previously configured on the router, the command is removed from the running configuration after the router is assigned as a neighbor to a BGP peer group.

Workaround: Re-enter the commands on the router.

- CSCeg52889

Symptoms: TE tunnels do not come up.

Conditions: This symptom is observed when a new loopback interface is created with an IP address on an MPLE TE head router that is configured with MPLS TE tunnels and when you reload the router. The symptom occurs because of a change in router ID.

Workaround: Shut down the newly created loopback interface, save the configuration, and reload the router.

- CSCeg54375

Symptoms: Routing inconsistencies may occur in the RIB: routes may be missing from the RIB but may be present in the BGP table.

Conditions: This symptom is observed on a Cisco RPM-XF when the toaster processor crashes. However, the symptom may occur on any platform that has a toaster processor.

Workaround: Enter the **clear ip route vrf vrf-name *** command.

- CSCeg70726

Symptoms: A router may crash when you enable MVPN by entering the **mdt default group-address** command under a VRF.

Conditions: This symptom is observed on a Cisco router that is configured for BGP VPNv4.

Workaround: There is no workaround.

- CSCeg85215

Symptoms: BGP may crash when a withdraw message is formatted.

Conditions: This symptom is observed on a Cisco router during the converge of peers.

Workaround: There is no workaround.

- CSCeg89700

Symptoms: A Cisco router does not recognize an end-of-RIB message from a third-party vendor router and continues to show the “Neighbor is currently in NSF mode” message although the restart procedure of the third-party vendor router is complete.

Conditions: This symptom is observed on a Cisco router that is configured for IPv6 BGP peering and NSF. Note that the symptom does not occur when IPv4 BGP peering is configured.

Workaround: There is no workaround.

- CSCeh07510

Symptoms: A traceback occurs on a router when you terminate an OSPF routing process by entering the **no router ospf** command.

Conditions: This symptom is observed when MPLS TE and more than one OSPF process are configured on the router.

Workaround: There is no workaround.

- CSCeh07809

Symptoms: When BGP nexthop information for a prefix changes because of topology changes, BGP properly updates its path information and IP routing table entry but CEF may not update the corresponding CEF entry, causing a stale entry. This inconsistency between BGP and CEF may cause a connectivity problem.

Conditions: This symptom is observed when the nexthop information changes to an existing prefix entry in the BGP routing table. Typically, this occurs when the interface through which the prefix is learned goes down.

Workaround: Flush out the stale CEF entry by entering the **clear ip bgp** command or withdraw and readvertise the prefix by the source router, which enables the affected router to refresh the CEF entry.

- CSCeh09588

Symptoms: During an NSF switchover on a RP, the convergence may be delayed up to five minutes.

Conditions: This symptom is observed when a DBD exchange error occurs while the adjacency is brought up.

Workaround: Enter the **clear ip ospf process** command on the affected router.

- CSCeh16989

Symptoms: The Multiprotocol BGP (MP-BGP) network entries counter increases above the real number of reachable networks.

Conditions: This symptom is observed when network activity occurs in a non-converged environment. The correct number of network entries is restored when there is a period of BGP stability that last for about 1 minute or more because BGP is able to converge and the scanner has time to run and collect the old network entries. However, if there is a sustained period of churn and BGP is only able to converge for a few seconds before new updates arrive, old BGP network entries are not cleaned up, causing the MP-BGP network entries counter to increase above the real number of reachable networks.

Workaround: There is no workaround.

- CSCin74330

Symptoms: The LDP Hello process may not be reinitiated after a TDP ID is received, preventing LDP neighbors from being discovered.

Conditions: This symptom is observed on a Cisco router that does not have an IP address configured when you first enter the **mpls ip** command and then assign the IP address.

Workaround: Assign the IP address to an interface of the router before you enable MPLS.

- CSCin87277

Symptoms: CPUHOG messages are generated when you bring up OSPF adjacencies on hundreds of subinterfaces.

Conditions: This symptom is observed when LSAs are configured to be refreshed every 30 minutes.

Workaround: There is no workaround.

- CSCsa40588

Symptoms: Routes may still appear in the routing table even after the routes are removed from the BGP table.

Conditions: This symptom is observed on a Cisco platform that functions as a PE router when a CE router stops advertising a BGP route to the PE router. The BGP table reflects the route change but the routing table still indicates that the route is valid.

Workaround: There is no workaround.

- CSCsa57101

Symptoms: A Cisco router may reload when the RSVP MIB object is polled via SNMP.

Conditions: The symptom is platform- and release-independent.

Workaround: Disable SNMP by entering the **no snmp-server host** command.

- CSCuk54787

Symptoms: When a route map is configured, routes may not be filtered as you would expect them to be filtered.

Conditions: This symptom is observed on a Cisco router that is configured for BGP and that functions in an MPLS VPN environment.

Workaround: There is no workaround.

ISO CLNS

- CSCef70231

Symptoms: When you enter the **no clns routing** command, adjacencies may be lost on any interface that is configured for IS-IS.

Conditions: This symptom is observed on a router that is configured for IS-IS and CLNS only when IS-IS is not specifically configured to route CLNS.

Workaround: Do not enter the **no clns routing** command when IS-IS is not specifically configured to route CLNS.

- CSCeh00090

Symptoms: Routes may be unexpectedly removed from the routing table.

Conditions: This symptom is observed when IS-IS is used to advertise IP prefixes and when you enter a **distance** command that changes the overall configuration but keeps a subset of the prefixes at the same distance as in the previous configuration. The routes for which the distance does not change may be removed from the routing table.

The following two examples show configurations in which the symptom occurs. When the distance configuration for IS-IS is **115 ip** and you enter one of the following command sequences, the symptom occurs:

```
router isis
```

```
distance 255 ip
```

```
distance 115 ip
```

or

```
router isis
```

```
distance 115 0.0.0.0 255.255.255.255
```

Workaround: For all prefixes, configure distances that differ from the distances that were initially configured.

- CSCeh00680

Symptoms: A router that is configured for Multi-Topology IS-IS (M-ISIS) may reload.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0S or Release 12.2S.

Workaround: Disable M-ISIS.

- CSCsa45381

Symptoms: CLNS fast-switching is disabled on a serial E3 interface that is configured for HDLC encapsulation.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(30)S but may also occur in other releases.

Workaround: There is no workaround.

Miscellaneous

- CSCdr54486

Symptoms: Traffic is dropped for up to 15 seconds while a recursive prefix is being resolved.

Conditions: This symptom is observed when a new recursive prefix is learned by CEF and when a less-specific prefix already exists. Traffic that would have been forwarded using the less-specific prefix is dropped for up to 15 seconds while the new recursive prefix is being resolved.

Workaround: There is no workaround.

- CSCdw00559

Symptoms: When you attempt to delete an entry from the ipNetToMediaTable table and if the associated ifIndex value is greater than the number of nonvirtual interfaces in the system, you cannot delete the entry successfully and receive a “WrongValue” error.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.1E but may also occur in other releases.

Workaround: There is no workaround.

- CSCec25942

Symptoms: A POS Engine 2 line card originates a high traffic volume to a downstream router over a POS link because the same packet is sent over and over.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(22)S5.

Workaround: There is no workaround.

- CSCec46954

Symptoms: A memory leak occurs when a subdirectory is created or extended.

Conditions: This symptom is observed in Cisco IOS Release 12.3 T (but may also occur in other releases) when any of the following actions are performed:

- You enter the **mkdir** command to create a subdirectory.
- You create a new file or you copy a file to disk.
- You create many files and directories under a subdirectory.

Workaround: If this is an option, do not use any subdirectory. Note that the symptom does not occur when you format a disk.

- CSCec51408

Symptoms: After you reload a Cisco 7xxx series router, the **vbr-nrt output-pcr output-scr output-mbs** command or the **ubr output-pcr** command may be missing from the configuration of the IMA-group interface of a PA-A3-8T1IMA or PA-A3-8E1IMA port adapter.

Conditions: The symptom is observed when the **vbr-nrt output-pcr output-scr output-mbs** command or the **ubr output-pcr** command is configured on an IMA-group interface that also has minimum active links configured.

Workaround: There is no workaround.

- CSCed57204

Symptoms: When a large number of VRFs are configured, input OAM F5 loopback cells on the ATM interface are dropped continuously, even without traffic. You can see drops at “OAM cell drops” in the output of the **show atm traffic EXEC** command and at “Input queue drops” in the output of the **show interface ATM EXEC** command.

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.2(19), Release 12.3(5), or Release 12.3(4)T2 when the **oam-pvc manage** and **ip vrf** global configuration commands are configured. The symptom may also occur in other releases.

Workaround: Remove the **ip vrf** command. There is no workaround for a router such as a provider edge (PE) router that cannot remove VRFs.

- CSCed95499

Symptoms: A Cisco router may crash if a PA driver attempts to convert an uncached iomem address to a cached iomem address.

Conditions: This symptom is observed on a Cisco 7200 series that is configured with an NPE-G1.

Workaround: There is no workaround.

- CSCee34622

Symptoms: Neighbor adjacencies for the IS-IS, OSPF, or other routing protocol may bounce during a Nonstop Forwarding (NSF) switchover.

Conditions: This symptom is observed when you enable a routing protocol for NSF and you enter the **external overload signalling** router configuration command. The following configuration illustrates this situation for IS-IS:

```
router isis area-tag
nsf [cisco | ietf]
external overload signalling
```

Workaround: Disable the **external overload signalling** router configuration command.

- CSCee49035

Symptoms: An incorrect update-source interface is selected for a multicast tunnel interface in an MVPN configuration.

Conditions: This symptom is observed when the provider edge (PE) router is also an ASBR with eBGP peers or has non-VPNv4 peers with higher IP addresses than the peer that has VPNv4 enabled. MVPN requires that the BGP update source address of a VPNv4 peer is selected as the MTI source address.

Workaround: There is no workaround.

- CSCee66058

Symptoms: SNMP users that have MD5 configured may become lost after a switchover in an RPR+ environment.

Conditions: This symptom is observed on a Cisco 7500 series and Cisco 12000 series that run Cisco IOS Release 12.0(27)S1 in RPR+ mode.

Workaround: There is no workaround.
- CSCee66214

Symptoms: A VIP may crash with a bus error after you have configured a multilink interface.

Conditions: This symptom is observed after you have configured a multilink interface with serial interfaces on a PA-MC-8TE1+ and PA-MC-8E1/120 port adapter.

Workaround: Use the same type of port adapter for each multilink interface.
- CSCee67278

Symptoms: A VIP may crash with a bus error and generate the following error message:

```
%ALIGN-1-FATAL: Illegal access to a low address
```

This occurs after the following scheduler error in the "req_proc" process:

```
%SYS-2-INTSCHED: 'sleep for' at level 2  
-Process= "req_proc", ipl= 2, pid= 27
```

Conditions: This symptom is observed on a Cisco 7500 series that runs a Cisco IOS image that contains the fix for CSCec07487 when a PA-MC-8TE1+ is installed in the VIP.

Workaround: There is no workaround.
- CSCee72906

Symptoms: A VIP may crash when you remove a service policy from a multilink interface or when a member link is removed from the multilink interface while heavy traffic is being processed.

Conditions: This symptom is observed on a Cisco 7500 series that has an RSP and that is configured for dLFI over a leased line, MLP, and QoS.

Workaround: There is no workaround.
- CSCee88296

Symptoms: A Cisco 12000 series reloads unexpectedly when you configure an MPLS TE tunnel.

Conditions: This symptom is observed when a PVC bundle is configured on an interface or subinterface and when you configure an MPLS TE tunnel on the same interface or subinterface.

Workaround: There is no workaround.
- CSCee91240

Symptoms: PRP crashes after you remove a port-channel interface.

Conditions: This symptom is observed on a Cisco 12000 series running that runs a Cisco IOS interim release for Release 12.0(30)S.

Workaround: There is no workaround.
- CSCef16379

Symptoms: An Engine 2 8-port ATM line card may not forward traffic from a VRF.

Conditions: This symptom is observed on a Cisco 12000 series when the prefix of the VRF is imported using an MPBGP tag.

Workaround: There is no workaround.

- CSCef16804

Symptoms: CEF entries for an adjacency that no longer exist are not purged.

Conditions: This symptom is observed when a large number of adjacencies is configured and when a switchover occurs.

Workaround: Enter the **clear cef linecard** command to purge the old entries.

- CSCef18515

Symptoms: After you have entered the **clear cef line** command, when you enter the **show ip cef** command for the RP and for a line card, the output is inconsistent.

Conditions: This symptom is observed on a Cisco 12000 series that runs a Cisco IOS interim release for Release 12.0(30)S and that is configured for Fast ReRoute.

Workaround: There is no workaround.

- CSCef22069

Symptoms: On a Cisco 12000 series that functions as an egress PE router in an MPLS VPN network, after the customer-facing Gigabit Ethernet line card is reloaded, the ingress line card that receives an incoming VPN label with a destination with a glean adjacency (which requires an ARP) without a BGP session may not properly complete the adjacency, causing traffic to be dropped.

Conditions: This symptom is mostly observed with static recursive route configurations. To recover from the symptom, manually ping the interface of the CE router from the adjacent PE router.

Workaround: Configure the static ARP entries for the nexthop router that is configured in the static recursive routes.

- CSCef25686

Symptoms: A number of PVCs may become locked in an inactive state, and the following type of error message may appear in the log:

```
%ATM-3-FAILREMOVEVC: ATM failed to remove VC(VCD=X, VPI=X, VCI=X) on Interface ATM X/X/X,
```

```
(Cause of the failure: PVC removal during recreation failed)
```

Conditions: This symptom is observed when you change the parameters of a VC class while the PVC is active and while you view the PVC status in the output of the **show atm vc interface interface-number** command.

The symptom occurs when you change the PVC speed in a VC class via one Telnet (or console) session and you enter the **show atm vc interface interface-number** command via another Telnet (or console) session.

Workaround: To remotely resolve the symptoms, remotely initiate an HA failover or remotely reload the affected router.

- CSCef25917

Symptoms: A 4GE-SFP-LC line card may reload unexpectedly when it processes QoS traffic in a configuration with a VLAN on a VCG that is configured with an ingress CoS.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(26)S or a later release when the resolved ARPs are deleted, for example, when routers flap, when BGP peers do not respond, or when you enter the **clear arp** command. Note that the symptom may also occur on releases earlier than Release 12.0(26)S.

The ingress CoS includes a **set** command for the matched class: either a **police** command with a **set** command or a simple **set** command and either a **set-mpls** command or a **set-dscp** command.

Possible Workaround: Configure static ARPs.

- CSCef26186

Symptoms: After a router reloads, Engine 0 POS and Engine 4+ POS line cards may reset because of an “%MDS-2-LC_FAILED_IPC_ACK” error.

Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of an interim release for Cisco IOS Release 12.0(30)S and that has multicast enabled in global configuration mode. Note, however, that this caveat is resolved in Release 12.0(30)S.

Workaround: There is no workaround.

- CSCef26543

Symptoms: A Cisco 12000 series line card may rate-limit process-switched packets to the GRP. This situation causes a ping to be lost when you perform a ping test to the local interface of the router.

Conditions: This symptom is observed when the interface is configured for HDLC, when the interface has a hard loop, and when the IP address of the interface is the destination of the ping. Because the interface is in the up/up state (looped) and functional, there should be no packet loss when you ping the interface at its own IP address.

Workaround: There is no workaround.

- CSCef30166

Symptoms: A Cisco router does not bring down a FR PVC when the interface on the ATM side is shut down.

Conditions: This symptom is observed on a Cisco router that runs an interim release for Cisco IOS Release 12.0(30)S only when OAM is configured on the ATM side.

Workaround: There is no workaround.

- CSCef30689

Symptoms: The AToM label holddown period is too short, and AToM traffic may be misdirected.

Conditions: AToM holds down its VC labels for 20 seconds before it releases them to the label manager. These labels are then available for allocation to other protocols or features such as LDP, TE, and MPLS VPNs. However, 20 seconds is not sufficient to guarantee that the AToM peer has properly deleted the entries and may cause AToM VC traffic to be misdirected by the protocol or features to which the freed AToM label is allocated.

Workaround: There is no workaround.

- CSCef35911

Symptoms: MPLS IAS traffic without labels is dropped at one ASBR when PPP encapsulation is configured between two ASBRs.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S1 and that functions as an ASBR. However, the symptom may be platform-independent and may also occur in other releases.

Workaround: Change the encapsulation to HDLC.

- CSCef41934

Symptoms: A router processes incoming LSP ping packets as unlabeled IP packets on a VRF interface or a non-MPLS interface.

Conditions: This symptom is observed on a Cisco router that has the MPLS LSP Ping feature enabled.

Workaround: Use an ACL to block port 3503 that is used for LSP ping packets. However, note that this may prevent some MPLS LSP Ping applications from functioning properly, as noted below:

LSP ping packets that enter on a VRF interface are dropped because the router uses the global routing table in its attempt to reply to MPLS echo requests, which could cause the reply to be forwarded to the wrong destination.

LSP ping packets that enter on an interface that is not configured for MPLS are processed, but depending on the type of MPLS echo packet, the following occurs:

- MPLS echo request packets are dropped.
- MPLS echo reply packets are not dropped. (It possible for an MPLS echo reply packets to be received on a non-MPLS interface because the reply path is asymmetric with the forward LSP.)

- CSCef49138

Symptoms: When you enter the **show policy-map interface interface-number** command, a router may crash because of a bus error exception.

Conditions: This symptom is observed on a Cisco 12000 series when the **service-policy output policy-map-name** command is enabled on the same interface for which you enter the **show policy-map interface interface-number** command.

Workaround: There is no workaround.

- CSCef49775

Symptoms: A PE router performs IP routing for untagged traffic that it receives from a CE router that is configured for L2VPN and VLAN.

Conditions: This symptom is observed on a Cisco 12000 series that functions as a PE router and that is configured for EoMPLS and VLAN. Note that you can reproduce the symptom with a single pseudowire.

Workaround: Configure an IP address on the main interface of the PE router and enter the **access-list access-list-number deny ip any any** command on the main interface.

- CSCef51239

Symptoms: When the MPLS LDP Graceful Restart feature is enabled, when label distribution protocol (LDP)-targeted sessions are configured, and when you globally disable LDP by entering the **no mpls ip** command while a graceful restart-enabled session is recovering, LDP may not be shut down properly.

When you then re-enable LDP by entering the **mpls ip** command, LDP may not allocate and advertise local labels for certain prefixes. When this situation occurs, MPLS connectivity may be interrupted because the router does not advertise a local label for certain prefixes.

Conditions: This symptom is observed when targeted sessions are requested to support AToM circuits and when the router runs Cisco IOS Release 12.2S, or a release that is based on Release 12.2S, that contains the fix for CSCed18355.

A list of the affected releases can be found at <http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCed18355>. Cisco IOS software releases not listed in the “First Fixed-in Version” field at this location are not affected.

Workaround: Clear the routes for the affected prefixes from the routing table by entering the **clear ip route EXEC** command. Note that the fix for this caveat is also integrated in Release 12.0S, 12.3, and 12.3T.

- CSCef53475

Symptoms: Packet drops occur when traffic is sent below the shape rate that is defined in a service policy.

Conditions: This symptom is observed on a Frame Relay interface when there are multiple DLCIs that have service policies enabled. Each DLCI has a hierarchical policy with a shape rate in the class default at the parent level and a child policy with LLQ and CBWFQ classes. When traffic to each DLCI is just below the shape rate and the combined traffic through the interface is close to line rate, packet drops occur on some DLCIs. The symptom does not occur when traffic is sent to one DLCI at the time.

Workaround: Increase the shape rate to compensate for the scheduling inaccuracy.

- CSCef55463

Symptoms: When you configure vbr-nrt shaping on two or more PVCs that are defined under the same physical ATM interface, one of the PVCs is subsequently unable to achieve the configured vbr-nrt rate.

Conditions: This symptom is observed when a PA-A3-8E1IMA or PA-A3-8T1IMA port adapter is installed in a Cisco 7xxx series and when the load is equal to or greater than the maximum configured vbr-nrt rate on at least two PVCs.

Workaround: Configure vbr-nrt rates proportionally higher on each PVC. Enter the **transmit-priority 1** command on the PVC that must reach the guaranteed vbr-nrt. Doing so causes the other PVC or PVCs to reach approximately 90 to 95 percent of the configured vbr-nrt rate.

- CSCef56201

Symptoms: Multicast MAC rewrites are not updated, preventing multicast traffic from being switched.

Conditions: This symptom is observed when the VLAN encapsulation is changed, for example from dot1q to dot1q, from dot1q to QinQ, or from QinQ to dot1q.

Workaround: Enter the **clear ip mroute** command.

- CSCef59275

Symptoms: Prefixes are rewritten over a FRR backup tunnel, causing traffic to drop from the tunnel.

Conditions: This symptom is observed when a point of local repair (PLR) runs Cisco IOS Release 12.0(29)S and the merge point (MP) runs a release earlier than Release 12.0(29)S or Release 12.2S.

Workaround: Run Release 12.0(29)S or a later release on the MP.

- CSCef59972

Symptoms: An RP crashes when you remove class maps from a policy map.

Conditions: This symptom is observed on a Cisco 12000 series that runs a Cisco IOS interim release for Release 12.0(30)S.

Workaround: There is no workaround.

- CSCef61641

Symptoms: A change in the controller state does not affect the subrate interface state.

Conditions: This symptom is observed on a Cisco 7500 series that is configured with an PA-MC-2T3+ port adapter.

Workaround: There is no workaround. However, you can synchronize the interface with the controller by entering the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface.

- CSCef61721

Symptoms: CEF may not be updated correctly with a route change.

Conditions: This symptom is observed when IPv6 BGP is configured and when a route changes from iBGP to eBGP or the other way around.

Workaround: Repopulate CEF with the correct forwarding information by entering the **clear ipv6 route** *ipv6-address* command.

- CSCef62335

Symptoms: A “VCID already in use” error message may be generated when you attempt to create an L2TPv3 session.

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.2S after you first have configured and removed a pseudo-wire configuration and then have removed the xconnect configuration from the PVC. The symptom may also occur in other releases.

Workaround: There is no workaround.

- CSCef63272

Symptoms: A recursive static default route may not have an outgoing MPLS label, causing all packets to be dropped.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(9) but may also occur in other releases.

Workaround: Add a nonrecursive static route to the BGP next-hop.

- CSCef66517

Symptoms: When you send larger than fragment-sized packets from an interface that has a traffic shaping class configured, the packets get stuck when the queue size increases to the queue limit, and subsequent traffic is tail-dropped.

Conditions: This symptom is observed when a policy is attached to a multilink interface that has a traffic shaping class configured and when the interface is configured for fragmentation.

Workaround: There is no workaround.

- CSCef67267

Symptoms: The Fast ReRoute database shows all prefixes in the active state.

Conditions: This symptom is observed on a Cisco router after a connected point of local repair (PLR) has rebooted.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface on which the primary tunnel is configured. Doing so restores the prefixes to the ready state.

- CSCef67840

Symptoms: When the CEF table consistency checker is configured to perform a passive scan check of tables of the line cards, the CEF table consistency checker may report false inconsistencies, which you can view in the output of the **show ip cef ip-address** command. The false inconsistencies may occur because of a race condition.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(27)S1.

If an inconsistency is reported for a recursive loadbalanced route for which the output interfaces for the next-hop IP address differ between the RP and line card, you can ignore this inconsistency because this information is not used during the forwarding process.

Workaround: Disable the CEF table consistency checker so that no passive scan check is performed of tables of the line cards.

- CSCef69066

Symptoms: The **set fr-fecn-becn** policy-map class configuration command may not take effect.

Conditions: This symptom is observed on a Cisco 7500 series.

Workaround: Enter the command again.
- CSCef70242

Symptoms: Low latency queueing (LLQ) and class-based weighted fair queueing (CBWFQ) may not function for MPLS packets. The MPLS packets that conform to the bandwidth that is allocated to these classes may be dropped.

Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2S when MPLS packets leave an interface that has an output policy map with **priority** or **bandwidth** commands, or both, configured within its classes. The symptom may also occur in other releases.

Workaround: There is no workaround.
- CSCef70566

Symptoms: After you have configured an ACL on a router to deny a traffic stream, traffic is shaped unexpectedly.

Conditions: This symptom is observed when the **no access-list** command fails while a nonvolatile generation (NVGEN) occurs.

Workaround: There is no workaround.
- CSCef70953

Symptoms: An Engine 4+ line card resets when you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on an interface of an Engine 3 Gigabit Ethernet (GE) line card in the same router.

Conditions: This symptom is observed on a Cisco 12000 series that functions in an EoMPLS configuration, that has an Engine 3 Gigabit Ethernet egress line card and an Engine 4+ core-facing line card, and that has CDP is enabled.

Workaround: Disable CDP.
- CSCef72411

Symptoms: Line cards and the standby RP on a Cisco 12000 series may fail when an RP switchover occurs.

Conditions: This symptom is observed on a Cisco 12000 series that runs a Cisco IOS interim release for Release 12.0(30)S and that has two PRPs when you enter the **redundancy force-switchover** command. Note that this caveat is resolved in Release 12.0(30)S.

Workaround: There is no workaround.

Further Problem Description: The fix for this caveat enables the RP to recover from a Fabric Interface ASIC (FIA) halt condition if this condition occurs following an RP switchover. In a Cisco IOS software release that does not integrate the fix for this caveat, the RP does not attempt to recover from a FIA halt condition after an RP switchover has occurred (but it does attempt to recover from such a conditions in other situations).
- CSCef77337

Symptoms: An IPv6 ACL is not properly applied to multiple interfaces.

Conditions: This symptom is observed on a Cisco 12000 series when an IPv6 ACL is applied to multiple interfaces (that is, four or more) and is modified to exceed layer 4 operating capabilities that can be supported in hardware.

Workaround: There is no workaround.

- CSCef78098

Symptoms: An Engine 1 or Engine 2 Gigabit Ethernet (GE) line card may stop switching traffic even though the line protocol is up. Pings and routing do not work, and traffic does not go through.

Conditions: This symptom is observed a Cisco 12000 series after error recovery and when the **negotiation auto** command is not configured for the interface of the GE line card.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface of the line card.

- CSCef79053

Symptoms: MFR interfaces may enter the “down/down” state following an RP SSO switchover.

Configuration: This symptom is observed on a Cisco 12000 series that has dual RPs that are configured in the hot standby SSO mode and occurs only when the router is configured with a line card that does not support SSO.

Workaround: There is no workaround.

- CSCef79749

Symptoms: APS does not function correctly on a channelized OC-48 ISE line card and the output of the **show aps** command shows that the line card is down.

Conditions: This symptom is observed on a Cisco 12000 series.

Workaround: There is no workaround.

- CSCef80349

Symptoms: An MPLS traffic engineering (TE) tunnel may not come back up after a link flaps.

Conditions: This symptom is observed when the headend of the TE tunnel is a third-party router that has the **no cspf** command configured for the label switched path (LSP) and when the tunnel midpoint is a Cisco router that runs Cisco IOS Release 12.0(25)S1. The symptom occurs when the link downstream (that is, towards the tailend of the tunnel) on the Cisco router fails because the interface on either side of the link is shut down.

In addition, note that the third-party router does not increment the LSP ID when it receives a message, nor does it send a PathTear message in response to a PathErr message.

Possible Workaround: Use an explicit path on the third-party router but without the **no cspf** command enabled.

- CSCef81555

Symptoms: The running configuration does not show the correct policing rate if the rate is configured to be larger than 4,200,000,000 bps.

Conditions: This symptom is observed on a Cisco 12000 series that runs an interim release for Cisco IOS Release 12.0(30)S.

Workaround: There is no workaround.

- CSCef82700

Symptoms: A 4-port Gigabit Ethernet (GE) line card generates TCAM errors when a large QoS configuration is applied. The following messages are generated:

```
%QM-2-TCAM_ERROR: TCAM pgm error(8): ACL Merge Failed
%QM-4-SW_SWITCH: Interface GigabitEthernet2/0 routed traffic will be software
switched in egress direction(s)
```

In addition, when you modify the policy map while it is still attached to the interface of the 4-port GE line card, the TCAM utilization goes up drastically; however, when you remove the policy map from the interface, the TCAM utilization is not brought back to zero.

Conditions: These symptoms are observed on a Cisco 12000 series when a child policy map with 75 or more customers is applied and when each child policy has at least 6 queues.

Workaround: Change the default merge algorithm to POD by entering the **hw-module slot slot-number reload** command for the slot in which the affected line card is installed.

Alternate Workaround: To avoid problems with the policy map modification, remove the service policy from the interface, modify the service policy, and reattach the service policy to the interface.

- CSCef83201

Symptoms: An interface does not return an RDI cell when it should do so but the ATM PVC statistics do increment to indicate that an RDI cell is returned.

Conditions: This symptom is observed when an F5 OAM Segment AIS is transmitted into an interface that has an ATM PVC (either a routed PVC or an l2transport PVC).

Workaround: There is no workaround.

- CSCef85231

Symptoms: When SSO redundancy mode is configured and you enter the **no** form of the **mpls ldp neighbor targeted** command to deconfigure a previously configured command, the standby RP may reload. The symptom may also occur when you enter the **no** form of the **mpls ldp neighbor implicit-withdraw** command. For example, any of the following command sequences may cause the symptom to occur:

Example 1:

```
mpls ldp neighbor 10.0.0.1 targeted ldp
...
no mpls ldp neighbor 10.0.0.1 targeted ldp
```

Example 2:

```
mpls ldp neighbor 10.0.0.1 targeted ldp
...
no mpls ldp neighbor 10.0.0.1 implicit-withdraw
```

Conditions: This symptom is observed when the **mpls ldp neighbor targeted** command is configured and when the Label Distribution Protocol (LDP) is globally disabled. (By default, LDP is globally enabled, but it can be disabled by entering the **no mpls ip** global configuration command.) The symptom does not occur when other commands are configured for the specific neighbor, for example, if an MD5 password is configured for the neighbor as illustrated in the command sequence below:

```
no mpls ip
mpls ldp neighbor 10.0.0.1 targeted ldp
mpls ldp neighbor 10.0.0.1 password foo
no mpls ldp neighbor 10.0.0.1 targeted ldp
```

This symptom occurs in releases that integrate the fix for caveat CSCee12408. A list of the affected releases can be found at

<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCee12408>.

Workaround: Configure a password for the neighbor as shown in the Conditions above before you enter the **no** form of the **mpls ldp neighbor targeted** command or the **no** form of the **mpls ldp neighbor implicit-withdraw** command.

- CSCef85916

Symptoms: In a scaled L2VPN configuration, CPUHOG-related tracebacks may be generated on a CE router.

Conditions: This symptom is observed on a Cisco 12000 series that runs the c12kprp-p-mz image of Cisco IOS Release 12.0(30)S and that functions as a CE router.

Workaround: There is no workaround.

- CSCef87309

Symptoms: A basic back-to-back ping fails on an Engine 4+ line card.

Conditions: This symptom is observed on a Cisco 12000 series that runs the c12kprp-p-mz image of a Cisco IOS interim release for Release 12.0(30)S. However, this caveat is resolved in Release 12.0(30)S.

Workaround: There is no workaround.

- CSCef89192

Symptoms: A self-ping may not function on a Cisco 12000 series and traffic may stop.

Conditions: This symptom is observed on a Cisco 12000 series after you remove and reconfigure a port-channel subinterface.

Workaround: Remove the member interfaces from the channel group and add them again. Doing so enables traffic to resume.

- CSCef89562

Symptoms: An Engine 4+ EPA-GE/FE-BBRD line card reports “%TX192-3-PAM_MODULE” and “%TX192-3-PAM_PIM” errors, and the interfaces continue to flap with the following error message:

```
%GRPGE-6-INVALID_WORD: Interface GigabitEthernet15/1/0: Detected RX Invalid Word
```

When there is heavy traffic, the line card may crash without generating any crashinfo.

Conditions: These symptoms are observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(26)S3 or Release 12.0(27)S3.

Workaround: There is no workaround.

- CSCef89925

Symptoms: IPv4 multicast traffic may be punted to the CPU of the RP, causing a throughput of only 700 pps.

Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of Cisco IOS Release 12.0(30)S.

Workaround: There is no workaround.

- CSCef90783

Symptoms: The output counter on the interface of a PE router that faces a P router generates almost twice the value that it should provide.

Conditions: This symptom is observed in the following MPLS topology in which Cisco 12000 series routers are connected via interfaces of Engine 3 line cards:

A CE router (CE1) connects to a PE router (PE1) that connects, in turn, to a P router. This P router connects to another PE router (PE2) that, in turn, connects to another CE (CE2) router.

The symptom occurs when a VRF ping is generated from PE1 to the VRF interface of PE2, that is, the interface that is connected to CE2. The output counter on PE2 generates incorrect values.

Workaround: There is no workaround.

- CSCef91030

Symptoms: After the default route is received from a remote PE for a VRF, communication stops for traffic via the default route in this VRF on a Cisco 12000 series that functions as a PE router in an MPLS VPN environment. The packets are switched out of the core MPLS interface untagged as native IPv4 packets instead of with MPLS and BGP labels.

Conditions: This symptom is observed when the traffic is received from VRF interfaces on an Engine 2 line card that is installed in a Cisco 12000 series that functions as a PE router.

The symptom occurs in Release 12.0(27)S2, Release 12.0(27)S3, and interim releases for Cisco IOS Release 12.0(30)S. Other releases may be affected too. The symptom does not occur in Release 12.0(24)S2.

The symptom occurs when the VRF ingress interface is configured on an Engine 2 3-port GE line card or Engine 2 1-port OC-48 POS line card. Other line cards may be affected too. The symptom does not occur when the VRF ingress interface is configured on a 4-port OC-3 POS Engine 0 line card or 4-port GE ISE line card.

Workaround: There is no workaround.

- CSCef91170

Symptoms: A Cisco 12000 series that has a CHOC12/DS1 ISE line card that is configured for mVPN over multilink PPP may not maintain PIM neighbors over GRE tunnels.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(27)S2, 12.0(27)S3, or 12.0(28)S1.

Workaround: On the multilink interface, enter the following sequence of commands:

```
Router(config)# interface multil
Router(config-if)# no ip pim sparse-dense-mode
Router(config-if)# ip pim sparse-dense-mode
```

Doing so enables the PIM neighbor to come up across the GRE tunnel.

- CSCef91475

Symptoms: A CPUHOG situation may occur intermittently on a Cisco 12000 series, causing fabric pipes to be lost and all OSPF and BGP adjacencies to be dropped.

Conditions: This symptom is observed in PRP on a Cisco 12000 series router.

Workaround: There is no workaround. However, the symptom resolves itself.

- CSCef92153

Symptoms: When a VRF VLAN subinterface punts a packet such as an ARP or ICMP packet to the CPU of the line card, the main interface is unable to process a packet such as ICMP packet that is destined for the main interface. When BGP packets enter and leave via the main interface, a BGP neighbor may go down.

These symptoms do not affect non-VRF subinterfaces, only the main interface. Transit packets that pass through the main interface are not affected.

When a non-VRF VLAN subinterface punts a packet to the CPU of the line card, the main interface may return to normal operational.

Conditions: These symptoms are observed on an Engine 4+ Gigabit Ethernet line card that is installed in a Cisco 12000 series that runs Cisco IOS Release 12.0 (25)S. Engine 2 and Engine 3 line cards are not affected. For the symptoms to occur, all of the following conditions must be present:

- A VRF VLAN subinterface is configured on the Engine 4+ line card.

- The main interface is also used with an IP address assigned to it.
- The VRF VLAN subinterface receives a packet such as an ARP or ICMP packet that is punted to the CPU of the line card.

For the BGP neighbor to go down, in addition to the above-mentioned conditions, the **neighbor ip-address password string** command must be configured.

Workaround: If you must use a VRF VLAN subinterface, create another subinterface for non-VRF communication on the same main interface.

Alternate Workaround: Do not use a VRF VLAN subinterface.

- CSCef93832

Symptoms: A router that reboots enters an infinite loop.

Conditions: This symptom is observed after a router has crashed and when the ROMMON does not gracefully recover during the rebooting process.

Workaround: There is no workaround.

- CSCef94525

Symptoms: A port adapter that is installed in a VIP or FlexWAN and that is configured with more than 38 multilink bundles may crash.

Conditions: This symptom is observed on a Cisco 7500 series and Cisco 7600 series when distributed CEF switching is disabled either through entering the **no ip cef distributed** command or through a FIB-DISABLE event.

Workaround: There is no workaround.

- CSCef94619

Symptoms: A VIP may crash while forwarding packets or a watchdog timeout crash may occur on the VIP during statistics collection.

Conditions: This symptom is observed on a Cisco 7500 series that is configured with an RSP4 and that runs Cisco IOS Release 12.0(26)S4.

Workaround: There is no workaround.

- CSCef96458

Symptoms: The OAM emulation status is displayed incorrectly.

Conditions: This symptom is observed when you enter the **show atm pvc** command.

Workaround: There is no workaround.

- CSCef96652

Symptoms: The offered rate counter in the output of the **show policy-map interface** command is inaccurate.

Conditions: This symptom is observed on a Cisco 12000 series when very high traffic rates are used.

Workaround: There is no workaround.

- CSCef97340

Symptoms: On an HA-capable router that is configured for distributed IPv6 multicast, the line cards may not perform distributed CEF switching of multicast traffic.

Conditions: This symptom is observed on a Cisco router that is configured with redundant RPs.

Workaround: There is no workaround for an HA-capable system. Removal of the RRP should restore proper operation by restoring the MRIB clients and MFIB tables on the line cards.

Further Problem Description: You can confirm the presence of the symptom for a router that is configured for distributed IPv6 multicast by entering the **show ipv6 mfib** command for the RP and line cards. The RP should correctly display the multicast forwarding table whereas the line cards should display the “Multicast Default Forwarding Table not found” error message.

- CSCef97533

Symptoms: A Cisco 12000 series may take a relatively long time to boot. This situation may cause traffic loss.

Conditions: This symptom is observed when you cold start a Cisco 12000 series that runs a Cisco IOS interim release for Release 12.0(30)S and that is configured with ISE line cards.

Workaround: There is no workaround.

- CSCef97536

Symptoms: When Multiprotocol Label Switching (MPLS) label distribution protocol (LDP) is configured and you enter the **clear ip route** EXEC command, the MPLS forwarding entries for some of the cleared routing prefixes may become unlabeled.

Conditions: This symptom is observed for prefixes that are connected (with an unspecified nexthop IP address) and that are not locally recognized. This situation may occur in a configuration in which two LDP peers are connected by a point-to-point link that uses PPP encapsulation, and in which both interfaces are configured to use IP addresses with /32 masks.

A list of the affected releases can be found at

<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCEe12379>. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

Possible Workaround: Prevent the symptom from occurring by using a shorter network mask when you configure the interfaces or by using another encapsulation such as HDLC.

When the symptom occurs, restore proper operation by forcing the LDP session that is associated with the link to re-establish itself, or by forcing the LDP session to re-advertise labels for the affected prefixes. The LDP session can be reset by entering the **clear mpls ldp neighbor** command, by administratively disabling and then re-enabling one of the interfaces, or by deconfiguring and then reconfiguring LDP on one of the interfaces. The LDP session can be forced to re-advertise labels by modifying the outbound label filtering configuration. However, this method is complicated and should only be attempted if you are already very familiar with the required procedures, and if the routers do not already have a complicated label filtering configuration in place.

- CSCef97964

Symptoms: A VIP4-80 crashes when you enter the **redundancy force-switchover** command.

Conditions: This symptom is observed on a Cisco 7513 that runs Cisco IOS Release 12.0(28)S1 and that is configured for SSO.

Workaround: There is no workaround.

- CSCeg00111

Symptoms: Padded IP fragments with an IP length that is shorter than 64 bytes and the More Fragments (MF) (which is set to 1) are dropped by an Engine 4+ line card that functions as an egress line card.

Conditions: This symptom is observed when the ingress line card is an Engine 4+ DPT line card and the egress line card is any Engine 4+ line card.

Workaround: There is no workaround.

- CSCeg00252

Symptoms: When you enter the **show sec-disk0:** command or the **execute-on slot slot-number command** command on the standby RP, no command output is generated.

Conditions: This symptom is observed on a Cisco 12000 series that has dual RPs and that is configured for RPR, RPR+, or SSO redundancy mode. Note that when you enter the **dir sec-disk0:** command on the standby RP, command output is properly generated.

Workaround: There is no workaround.
- CSCeg01168

Symptoms: Counters that are displayed in the output of the **show interface** commands for an ATM interface of an 8-port OC3 ATM line card show incorrect input packet and byte counts.

Conditions: This symptom is observed on a Cisco 12000 series when the Port Mode Cell Relay Support feature is configured on the ATM interface.

Workaround: There is no workaround.
- CSCeg01543

Symptoms: A Cisco 7500 series VIP may crash when its serial interfaces are part of a Multipoint Frame Relay (MFR) bundle.

Conditions: This symptom is observed when a Frame Relay end-to-end fragment is received on an MFR interface.

Workaround: Administratively shut down the MFR interface or shut down the MFR interface on the other side of the link.
- CSCeg01740

Symptoms: A router crashes when you delete a manual static Xconnect service with L2TPv3 encapsulation.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0S but could also occur in other releases.

Workaround: Do not delete a manual static Xconnect service with L2TPv3 encapsulation.
- CSCeg02016

Symptoms: The OSPF process may be down for link-bundling subinterfaces.

Conditions: This symptom is observed on a Cisco 12000 series that is configured with two RPs and that runs Cisco IOS Release 12.0(30)S when the redundancy mode is set to SSO.

Workaround: Change the redundancy mode to RPR.
- CSCeg03055

Symptoms: Sampled NetFlow may stop functioning.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(23)S3 or a later release and that is configured with an Engine 4 plus 4-port OC-48 line card when the hardware of the line card is reset as a result of an error recovery process.

Workaround: Disable and re-enable Sampled NetFlow.
- CSCeg03180

Symptoms: A line card in slot 15 is stuck in the WAITRTRY state.

Conditions: This symptom is observed on a Cisco 12816 that is configured with dual RPs when an RP switchover followed by a CSC switchover occurs.

Workaround: Reload the router.

Alternate Workaround: Power down and power up the router.

- CSCeg03606

Symptoms: Multicast VPN (MVPN) traffic does not resume.

Conditions: This symptom is observed on a Cisco 12000 series that runs a Cisco IOS interim release for Release 12.0(30)S and that functions as a PE router that is configured for MVPN.

Workaround: Enter the **clear ip mroute** command.

- CSCeg03885

This caveat consists of two symptoms, two conditions, and two workarounds, and only refers to routers that are configured with MPLS TE tunnels:

Symptom 1: Momentary packet loss may occur during tunnel reoptimization, usually several times between the creation of a new tunnel and the cleanup of the old tunnel. Sometimes, longer packet loss may occur during tunnel reoptimization.

Condition 1: This symptom is observed on any MPLS TE tunnel when the reoptimized label switched path (LSP) traverses a midpoint or headend router that runs Cisco IOS Release 12.0(25)S4.

Workaround 1: There is no workaround.

Symptom 2: Permanent bad labels may be present after MPLS TE tunnel reoptimization.

Condition 2: This symptom is observed on a router that runs a Cisco IOS image that does not include the fix for CSCed21063 and that functions in a network in which some routers run Cisco IOS Release 12.0(25)S4. With the exception of release 12.0(25)S4 itself, Cisco IOS software releases that are listed in the “First Fixed-in Version” field at the following location are not affected:
<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCed21063>.

Workaround 2: There is no workaround. To recover from the symptoms, enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected TE tunnel interface.

- CSCeg05681

Symptoms: A CSC OIR may cause all line cards in a router to enter the disabled state and the standby RP to reload continuously.

Conditions: The symptom is observed on a Cisco 12000 series that has dual PRPs and that runs a Cisco IOS interim release for Release 12.0(30)S.

Workaround: There is no workaround.

- CSCeg05925

Symptoms: After you have entered the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on a VLAN interface, MPLS traffic is dropped.

Conditions: This symptom is observed only when MPLS static labels are configured. When an MPLS TFIB entry is created using MPLS static labels and when you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the egress VLAN interface, the MPLS entry may be missing from the TFIB on the line cards or port adapters.

Workaround: Enter the **clear ip route** command for the affected prefix.

- CSCeg06154

Symptoms: A router crashes when you delete an MPLS subinterface by entering the **no interface** command.

Conditions: This symptom is observed when the **mpls ip** command is configured on the same MPLS subinterface. For example, consider a router with the following configuration:

```
interface atm1/0.1 mpls
  mpls ip
```

When you enter the **no interface atm1/0.1 mpls** command, the router crashes.

Workaround: There is no workaround.

- CSCeg06618

Symptoms: A 6-port channelized T3 line card and a 2-port Channelized OC-3 line card may continuously generate the following error message:

```
%LC_CX3-2-PLIM_CPU_CRASHED: PLIM CPU Tofab755 - plim reset
```

Controllers and interfaces do not recover.

Conditions: This symptom is observed on a Cisco 12000 series and occurs because of a problem with the recovery mechanism following a forced reset of the PLIM component of the line card. The symptom is visible only if another problem indirectly triggers a forced reset of the PLIM component.

Workaround: There is no workaround. To recover the affected line card, reload the line card by entering **hw-module slot slot-number reload** command.

- CSCeg07296

Symptoms: When you configure an AToM pseudowire, a memory allocation failure occurs followed by data corruption.

Conditions: This symptom is observed on a Cisco 12000 series.

Workaround: There is no workaround.

- CSCeg08629

Symptoms: A Cisco 7500 series may generate CCB playback errors and reload the secondary Route Switch Processor (RSP).

Conditions: This symptom is observed when there are channelized T3 port adapters installed in the router and when a channel-group parameter is configured before the channel group is created. To recover from the symptoms, reload the router.

Workaround: Configure the channel-group via the **t1 t1-line-number channel-group channel-group-number timeslots list-of-timeslots** command before you configure any options such as framing of FDL on the channel group.

- CSCeg09141

Symptoms: Sampled NetFlow stops functioning.

Conditions: This symptom is observed on a Cisco 12000 series that is configured with a 4-port OC-48 line card.

Workaround: Disable and then re-enable Sampled NetFlow.

- CSCeg10276

Symptoms: A routing loop occurs when you enter the **mpls traf-eng tunnel reoptimize** command on a PRP.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S1 and that is configured with an Engine 3 line card through which traffic enters and leaves.

Workaround: Enter the **clear cef linecard** command on the interfaces that are affected by the routing loop.

- CSCeg11421

Symptoms: A Cisco 10720 crashes when you delete an IPv6 ACL.

Conditions: This symptom is observed when you delete the IPv6 ACL during the TurboACL compilation.

Workaround: Wait for the ACL to be fully compiled before you delete it.

- CSCeg11513

Symptoms: When a Label Distribution Protocol (LDP) session flaps, error messages similar to the following may be generated:

```
%TAGCON-3-PEERSM: TDP peer 10.1.3.55(172.16.1.1:0):
multiple deferred adjs
%TAGCON-3-PEERSM: TDP peer 10.1.3.54(172.17.1.1:0):
multiple deferred adjs
```

In most cases, these messages do not affect the LDP functions. However, when an Any Transport over MPLS (AToM) VC is configured over the LDP session, the AToM VC may stay in the down state.

Conditions: These symptoms are observed when Multiprotocol Label Switching (MPLS), LDP, and MLS LDP Graceful Restart are enabled.

Workaround: Disable MLS LDP Graceful Restart.

- CSCeg11773

Symptoms: The active RP crashes when you perform a microcode reload of the line cards while the standby RP is booting.

Conditions: This symptom is observed on a Cisco 12000 series that runs a Cisco IOS interim release for Release 12.0(30)S and that is configured for RPR.

Workaround: There is no workaround.

- CSCeg13308

Symptoms: An Engine 6 line card may reset when line card error recovery is invoked.

Conditions: This symptom is observed on a Cisco 12000 series router that runs the gsr-p-mz image of Cisco IOS Release 12.0(30)S.

Workaround: There is no workaround.

- CSCeg13868

Symptoms: When the **no tag-switching ip propagate-ttl** command is configured on PE routers and a traceroute is executed from one CE router to a remote CE router, an egress PE router replies to the traceroute with the address of its ingress MPLS interface.

Conditions: This symptom is observed only when the traceroute is destined for a network between an egress PE router and a remote CE router, when the ingress line card of the egress PE router is a Cisco 12000 series Engine 0 or Engine 1 line card.

Workaround: There is no workaround.

- CSCeg13924

Symptoms: When an Engine 0 2-port channelized OC-3 line card comes up after you have reloaded the microcode, the E1 interface and controllers come up and the DLCI for an Xconnect service across an MPLS comes up, but the locally switched DLCI for the Xconnect service is down (the state is "OPER DOWN" and the DLCI is inactive).

Conditions: This symptom is observed on a Cisco 12000 series that runs the k4p-mz image of a Cisco IOS interim release for Release 12.0(30)S. However, this caveat is resolved in Release 12.0(30)S.

Workaround: Bring up the locally switched DLCI by deleting and reconfiguring the **xconnect** command.

- CSCeg15191

Symptoms: An OC192E/POS-IR-SC line card resets with the following error messages:

```
%MBUS_SYS-3-NOBUFFER: Message from slot 3 in stream 1 dropped
```

```
%MDS-2-LC_FAILED_IPC_ACK: RP failed in getting Ack for IPC message of size 232 to LC in slot 3 with sequence 47350, error = timeout
```

```
%FIB-3-FIBDISABLE: Fatal error, slot 3: IPC Failure: timeout
```

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S1.

Workaround: There is no workaround.

- CSCeg16739

Symptoms: A Cisco 10720 crashes when you add and remove a large IPv6 ACL very quickly.

Conditions: This symptom is observed only on a Cisco 10720 that has a large 500-line ACL while the ACL is compiling.

Workaround: Wait until the ACL has compiled before you remove the ACL.

- CSCeg16790

Symptoms: A policy map that causes AAL5 IP to enable the **set precedence 4** command does not function. Note that a policy map that causes ATM to enable the **set mpls experimental imposition** works fine.

Conditions: This symptom is observed on a Cisco 12000 series Engine 2 8-port OC-3 ATM line card when a policy map is configured on a PVC that performs Layer-3 forwarding of AAL5 packets.

Workaround: There is no workaround.

- CSCeg19298

Symptoms: A router may crash when you enter the **show running-config** command.

Conditions: This symptom is observed when a bundle is configured on an ATM interface and when you enter the **show running-config** after you have entered the **no protocol protocol-address** command for the bundle.

Workaround: There is no workaround.

- CSCeg20700

Symptoms: When an Engine 2 ATM line card is configured with the Carrier Supporting Carrier feature and egress traffic is being processed, the following error message may be generated on the line card and the line card may reset:

```
%QM-4-STUCK: Port 2 Queue mask 0x1
```

Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of a Cisco IOS interim release for Release 12.0(31)S. However, this caveat is resolved in Release 12.0(31)S.

Workaround: There is no workaround.

- CSCeg20771

Symptoms: During intense interaction between the RP and line cards, the RP may crash because of a corruption. This symptom occurs when large numbers of VRFs are continuously created and deleted. However, the trigger for the symptom to occur could be caused by something else.

Conditions: This symptom is observed on a Cisco 12410 that is configured with about 100 VRFs and that runs Cisco IOS Release 12.0(27)S2, 12.0(28)S1, or an interim release for Release 12.0(29)S. The symptom is not observed in Release 12.0(30)S.

Workaround: Do not add or delete more than VRFs at one time.

- CSCeg21548

Symptoms: A router crashes when you enter the **show bfd neighbors** command.

Conditions: This symptom is observed on a Cisco platform while BFD sessions flap.

Workaround: There is no workaround.

- CSCeg25493

Symptoms: Several VIPs may crash at about the same time because of a bus error.

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(26)S4 and that is configured with an RSP4 when the VIPs are configured for QoS but have insufficient memory.

Workaround: Increase the amount of memory on the VIPs.

- CSCeg28402

Symptoms: Spurious memory accesses may occur on a Cisco 7500 series and may cause high CPU usage on the RSP.

Conditions: This symptom is observed on a Cisco 7500 series that is configured for distributed Multilink PPP (dMLP) and that functions in an MPLS network.

Note that packet switching for MPLS packets over MLP bundles is not supported at the RSP level in Cisco IOS Release 12.0S.

Workaround: There is no workaround.

Further Problem Description: The fix for this caveat causes packets that are sent to the RSP for switching to be dropped. Distributed forwarded packets are forwarded correctly.

- CSCeg29995

Symptoms: A router crashes when you create an IPv6 static neighbor entry that replaces an incomplete ND cache entry and when you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command multiple times on the interface that connect to the neighbor.

Conditions: This symptom is observed when the following events occur:

1. The router receives and attempts to forward packets to a non-responding IPv6 neighbor, causing the router's ND cache entry for the IPv6 neighbor to be in the incomplete (INCMPL) state.
2. You create a static neighbor entry by entering the **ipv6 neighbor** command for the same (non-responding) neighbor.
3. You enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command multiple times on the interface on which the static neighbor entry is defined, or the interface is shut down and the static neighbor is deleted.

Workaround: Ensure that the IPv6 static neighbor is manually created before the processing of traffic causes an incomplete ND cache entry to be created for the same neighbor.

- CSCeg31430

Symptoms: A memory leak may occur on a router that has rate-limiting configured.

Conditions: This symptom is observed when the router is configured with two mutually exclusive exceed statements as in the following example:

```
Router#sh run | b <name>
policy-map <name>
  class <classname>
    bandwidth 50
    random-detect
    random-detect exponential-weighting-constant 3
    random-detect precedence 0 3 9 1
    random-detect precedence 7 3 11 1
  police cir 50000 bc 8000 pir 119000 be 16000
    conform-action transmit
    exceed-action transmit
    exceed-action set-prec-transmit 0
    violate-action drop
  queue-limit 22
```

Workaround: To stop the memory leak, delete one of the exceed statements.

- CSCeg31912

Symptoms: Ingress policing and bandwidth percent per-class do not function and limit traffic at the configured bandwidth for MLFR links. The output of the **show policy-map interface** command shows the configured bandwidth which differs from the actual bandwidth.

Conditions: This symptom is observed on a Cisco 7500 series after the router is reloaded.

Workaround: Remove the service policy and re-apply it to interface to enable correct calculation of the interface bandwidth.

- CSCeg33229

Symptoms: A VIP may crash when an ingress service policy is removed from an MFR interface.

Conditions: This symptom is observed on a Cisco 7500 series while traffic is being processed on the MFR interface.

Workaround: There is no workaround.

- CSCeg35517

Symptoms: An Engine 3 1-port OC-12 channelized DS1 line card that is configured for MLP may reset or may cause the RP to reset.

Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of Cisco IOS Release 12.0(31)S.

Workaround: There is no workaround.

- CSCeg37524

Symptoms: A 4-port OC-12 ATM single mode (4OC12/ATM-IR-SC) line card may generate unicast send timeout errors, %LC-3-PSAERRS errors, and %LC-3-BMAERRS errors, which cause TDP neighbor flapping and may cause the line card to crash.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(27)S3.

Workaround: There is no workaround.

- CSCeg38266

Symptoms: After a router reloads, distributed multicast switching becomes disabled on interfaces of a 1-port channelized OC-12/STM-4 (DS1/E1) ISE line card that have the **ip mroute-cache** command configured in the startup configuration.

Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of Cisco IOS Release 12.0(28)S1.

Workaround: After the router has reloaded, re-enter the **ip mroute-cache** command for the affected interfaces.

- CSCeg40957

Symptoms: A router that is equipped with a PA-A3-OC3 ATM port adapter may generate alignment errors.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(25)S1 and that is configured for Xconnect.

Workaround: There is no workaround.

- CSCeg41152

Symptoms: MLP interfaces on an Engine 3 1-port channelized OC-12 DS1 line card do not forward traffic.

Conditions: This symptom is observed on a Cisco 12000 series.

Workaround: There is no workaround.

- CSCeg44261

Symptoms: A memory leak may occur in the Segment Switch Manager (SSM) connection manager process.

Conditions: This symptom is observed only on a Cisco platform that supports hardware switching for all sessions that use the SSM, including AToM, L2TPv2, L2TPv3, PPP, and PPPoE. When a session is terminated or unconfigured, SSM-related memory is not freed.

Workaround: There is no workaround.

- CSCeg44426

Symptoms: A Cisco 12000 series denies traffic that matches the L3 information of an ACE that is configured with the **undetermined-transport** keyword.

Conditions: This symptom is observed on a Cisco 12000 series that performs IPv6 ACL filtering in hardware.

Workaround: There is no workaround.

- CSCeg44491

Symptoms: MFR Xconnect does not come up and the following error message and traceback are generated:

```
%SW_MGR-3-CM_ERROR: Connection Manager Error - unprovision segment failed
[SSS:FR:356438] - no private context found.

-Traceback= 60FA8C28 60FA8D2C 6049715C 60FA6CC4 60FAF7D4 60FA6E70 60FA7050 60FA4DE0
60FAF7D4 60FA5120 60FA2C84 60FA2CE4 60FA412C 60FA4394
```

Conditions: This symptom is observed on a non-distributed Cisco platform such as a Cisco 7200 series when you attempt to configure Xconnect on an MFR interface.

Workaround: There is no workaround.

- CSCeg45888
Symptoms: You cannot ping a global IPv6 address from a dual-mode IEEE 802.17 RPR/SRP uplink module.
Conditions: This symptom is observed on a Cisco 10720.
Workaround: There is no workaround.
- CSCeg49685
Symptoms: An exception occurs on a line card and the line card resets.
Conditions: This symptom is observed when you create a Frame Relay subinterface for a channel with a high channel number such as 800.
Workaround: Do not create a Frame Relay subinterface for a channel with a channel that is higher than 723.
- CSCeg50491
Symptoms: The RP of a Cisco 12000 series crashes and the router reloads.
Conditions: This symptom is observed on a Cisco 12000 series that is configured with a 1-port channelized OC-12/STM-4 (DS1/E1) ISE line card when you reload this line card after you have repeatedly deleted and re-added interfaces while the OC-12 link is flapping.
Workaround: There is no workaround.
- CSCeg51793
Symptoms: When you delete an IP VRF by entering the **no ip vrf** *vrf-name* command and you attempt to reconfigure the IP VRF before it is completely deleted, an address error exception may occur.
Conditions: This symptom is observed on a Cisco platform that is configured for MVPN.
Workaround: Wait until the IP VRF is completely deleted: enter the **show ip vrf** command to verify that the IP VRF is deleted before you reconfigure it.
- CSCeg53483
Symptoms: When you enter the **show running-config** command, a traceback may be generated because of a CPU hog condition.
Conditions: This symptom is observed when large number of class maps (2500) is configured.
Workaround: There is no workaround.
- CSCeg56488
Symptoms: After you perform a microcode reload on an Engine 0 or Engine 3 channelized line card that is configured for VPN on a Frame Relay subinterface or dot1q subinterface, you can no longer ping a directly connected interface and traffic does not go through.
Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of Cisco IOS Release 12.0(31)S.
Workaround: There is no workaround.
- CSCeg61532
Symptoms: BGP does not come up after you have reloaded microcode onto a 4-port Gigabit Ethernet ISE line card.
Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of an interim release for Cisco IOS Release 12.0(31)S.
Workaround: There is no workaround.

- CSCeg65439
Symptoms: A Cisco 12000 series may hang while reloading.
Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz or c12kprp-p-mz image of an interim release for Cisco IOS Release 12.0(31)S.
Workaround: There is no workaround.
- CSCeg66282
Symptoms: The controller of a 1-port multichannel STM-1 port adapter (PA-MC-STM1) does not come up after the router has reloaded.
Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(28)S2.
Workaround: There is no workaround.
- CSCeg66627
Symptoms: An Engine 6 line card may reset because of an IPC timeout and may generate the following error message:

```
%MCC192-3-CPUIF_ERR: Packet Exceeds Programmed Length
```


Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(27)S3.
Workaround: There is no workaround.
- CSCeg67495
Symptoms: A VIP may crash because of a bus error.
Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(29)S and that is configured for QoS.
Workaround: There is no workaround.
- CSCeg69381
Symptoms: When you perform a physical OIR or you reload microcode on a line card that is installed in slot 15, Engine 6 line cards in other slots of the chassis are reset and CEF failure messages are generated. This situation affects traffic and routing updates.
Conditions: The symptom is observed on a Cisco 12000 series. When you perform a physical OIR or you reload microcode on a line card that is installed in a slot other than slot 15, the symptom does not occur.
Workaround: There is no workaround.
- CSCeg69991
Symptoms: A basic ping between two Engine 3 imposition line cards that are configured for PPP or HDLC transport does not function.
Conditions: This symptom is observed on a Cisco 12000 series that runs an interim release for Cisco IOS Release 12.0(31)S when PPP or HDLC encapsulation are configured over MPLS.
Workaround: There is no workaround.
- CSCeg73965
Symptoms: Channelized interfaces may remain down after you delete and reconfigure a large configuration. The interfaces may report an LOF alarm.
Conditions: This symptom is observed on a Cisco 12000 series that is configured with point-to-point channelized interfaces.

Workaround: Reload the router to enable the interfaces to come into service.

- CSCeg74271

Symptoms: In some cases, when changing the IP address of the PGP link in an MR- APS configuration, the router may pause indefinitely.

Conditions: This symptom was observed on a Cisco 12000 router running Cisco IOS Release 12.0(30)S. This symptom also affects other Cisco router families running Cisco IOS Release 12.0(30)S.

Workaround: There is no workaround.

- CSCeg76331

Symptoms: There may be an incomplete adjacency on a PE router for the IP address of the Gigabit Ethernet interface of a locally-connected next-hop CE router and there may be an incomplete ARP entry for the next-hop CE router in the VRF ARP cache of the PE router.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(30)S, that functions as a PE router with static routes that are configured within the VRF, and that has a 4-port Gigabit Ethernet line card as the egress line card.

The symptom occurs when a packet is lost when traffic is sent from a remote CE or PE router and when you enter the **shutdown** command followed by the **no shutdown** command on the VRF interface of the Cisco 12000 series.

Workaround: From the Cisco 12000 series, ping the interface of the locally-connected next hop CE router. Doing so populates the ARP cache and enables the incomplete adjacency to become complete and valid.

- CSCeg79456

Symptoms: An Engine 6 line card may reset because of an IPC timeout.

Conditions: This symptom is observed on a Cisco 12816 that runs Cisco IOS Release 12.0(27)S4 when you enter the **shutdown** command on the primary Clock Scheduler Card (CSC) or you enter the **no shutdown** command on the secondary CSC that is in the shut down state.

Workaround: There is no workaround.

- CSCeg83399

Symptoms: When an ATM PVC is configured with an egress service policy, exiting from the PVC configuration mode by entering the **exit** command may cause traffic that is forwarded from other PVCs on the line card to be dropped.

Conditions: This symptom is observed on a Cisco 12000 series router that is configured with an ATM ISE line card or an 8-port OC-3 ATM Engine 2 line card.

Any action that causes the affected ATM PVC to be reinitialized restores traffic forwarding.

Workaround: Do not enter the **exit** command to exit from the PVC configuration mode. Rather, enter the **end** command.

- CSCeg83614

Symptoms: A router that has MPLS traffic engineering tunnels and that is configured for Fast ReRoute may crash because of memory corruption.

Conditions: This symptom is observed only on a Point of Local Repair when a primary tunnel has bandwidth protection enabled via the **tunnel mpls traffic-eng fast-reroute bw-protect** command and when more than eight LSPs are pre-empted to make room for the bandwidth-protected LSP.

Workaround: There is no workaround.

- CSCeg84057
Symptoms: Unchannelized interfaces do not stay in service after their initial configuration.
Conditions: This symptom is observed on a Cisco 12000 series when the interfaces are configured for PPP.
Workaround: There is no workaround.
- CSCeg84224
Symptoms: Line cards are shut down by the environmental monitor and the following error message is generated:

```
%ENV_MON-2-VOLTAGE: PLIM V6 -5v supply(slot 1) volts has reached SHUTDOWN level at 602 61 m(V)
%ENV_MON-1-SHUTDOWN: Environmental Monitor initiated shutdown on slot# 1
```


The line cards initially come up into the IOS-RUN state, but then enter the OFF-PWR state because they are shut down by the environmental monitor. Performing an OIR or entering the **microcode reload** command does not bring the line cards back up
Conditions: This symptom is observed on a Cisco 12816 that runs a Cisco IOS interim release for Release 12.0(31)S and that is configured with an Engine 6 OC-192 POS line card.
Workaround: There is no workaround.
- CSCeg86187
Symptoms: The **ip mroute-cache distributed** interface configuration command is not retained after you reload a router.
Conditions: This symptom is observed on a Cisco 7500 series.
Workaround: After the router has reloaded, reconfigure the **ip mroute-cache distributed** interface configuration command on each affected interface.
- CSCeg88402
Symptoms: Local switching between an Auto-VC and a VC fails. The output of the **show connect** command shows “OPER DOWN”.
Conditions: This symptom is observed when you enter the **connect** legacy command (as opposed to the current **xconnect** command) to set up local switching between an Auto-VC and a VC.
Workaround: Use VCs instead of Auto-VCs.
- CSCeg88655
Symptoms: A RP switchover causes %SYS-2-NOTQ and %SYS-2-LINKED errors and some tracebacks on a Cisco 12000 series 1-port channelized OC-12c/STM-4 (DS1/E1) ISE line card.
Conditions: This symptom is observed on a Cisco 12000 series dual-PRP router that runs a Cisco IOS interim release for Release 12.0(31)S.
Workaround: There is no workaround.
- CSCeg88806
Symptoms: Disabling the **mpls ip** command while a router attempts to establish a Label Distribution Protocol (LDP) connection with some peers after having failed to do so may cause the router to crash with an error message that is similar to the following:

```
%SYS-2-FREEFREE: Attempted to free unassigned memory at 445F4DAC, alloc 40C7A4F0,
dealloc 40C7A3A4
-Traceback= 403295F4 403E907C 40C7A3AC 40C60BD0 40C92F80 40C8E06C 403CF458 403CF444
```

Conditions: This symptom is observed on a Cisco router that is configured for Multiprotocol Label Switching (MPLS) LDP and that has failed to establish an LDP session with some peers.

Workaround: Configure Tag Distribution Protocol (TDP) as the MPLS label protocol.

- CSCeg88815

Symptoms: A PRP crashes after you remove a PVC from a main interface of a 4-port OC-12 ATM ISE line card that has an outbound service policy enabled.

Conditions: This symptom is observed on a Cisco 12406 that runs a Cisco IOS interim release for Release 12.0(31)S and that is configured with redundant PRPs when you remove a PVC with a "255/255" configuration.

Workaround: There is no workaround.

- CSCeg89117

Symptoms: A segment base is not freed, causing a memory leak.

Conditions: This symptom is observed when you unconfigure xconnect over an L2TPv3 connection.

Workaround: There is no workaround.

- CSCeg89202

Symptoms: When you attach a policy with a priority class to a subinterface of a channelized OC-48/STM-16 (DS3/E3, OC-3c/STM-1c, OC-12c/STM-4c) POS/SDH ISE line card that is configured with Frame Relay subinterfaces, the default queue limit for the priority queue of the port changes to a value that is calculated by the policy map that was attached. This situation causes QoS to be impacted.

Conditions: This symptom is observed on a Cisco 12000 series.

Workaround: Ensure that the policy map that you attach last calculates the desired queue limit, which is then applied to all subinterfaces of the port.

- CSCeh00169

Symptoms: After you have reloaded a router, for each of the service policies that are attached to the interfaces of a 4-port OC-12 POS ISE line card, the policing of L2 VCs may fail when errors with the following associated error messages occur:

"Must remove existing service policy first .."

or

"Configured exceed actions are not supported when policing L2 VCs on interface.."

When the policing of L2 VCs fails, the following error message is generated:

"L2 policing config failed."

Conditions: This symptom is observed on a Cisco 12416 that runs the c12kprp-p-mz image of a Cisco IOS interim release for Release 12.0(31)S and that is configured with dual PRPs and 4-port OC-12 POS ISE line card that has a service policy attached to each of its interfaces.

Following are examples of configurations that may trigger the symptoms:

```
policy-map testing-input
class class-default
  police cir percent 2 pir percent 4
  conform-action set-mpls-exp-imposition-transmit 4
  exceed-action set-mpls-exp-imposition-transmit 1
  violate-action drop
!
```

```

map-class frame-relay testing
  service-policy input testing-input

interface POS6/0
  frame-relay interface-dlci 17 switched
  class testing

```

Workaround: There is no workaround.

- CSCeh01992

Symptoms: A Cisco 12000 series crashes after you enter a PVC configuration with an xconnect statement on a subinterface for a 4-port OC-12 ATM ISE line card that has AAL5SNAP encapsulation enabled.

Conditions: This symptom is observed on a Cisco 12406 that is configured with a single 1 GRP-B and that runs a Cisco IOS interim release for Release 12.0(31)S.

Workaround: There is no workaround.

- CSCeh02579

Symptoms: A multilink bundle on a Cisco 10000 series may lock up. The multilink bundle may transmit packets but does not process any incoming packets, indicating that all links of the bundle are in an out-of-order state and draining.

Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.0(25)SX, Release 12.0(26)S4, or a later 12.0S release and that is configured for mVPN and MLP. The symptom may be platform-independent.

Workaround: If this is an option, disable mVPN.

- CSCeh04991

Symptoms: In a scaled configuration with 2500 customer connections, a standby RP may crash after a router reloads.

Conditions: This symptom is observed on a Cisco 12416 that runs the c12kprp-p-mz image of a Cisco IOS interim release for Release 12.0(31)S and that is configured with dual PRPs.

Workaround: There is no workaround.

- CSCeh05594

Symptoms: A router configured for Fast ReRoute (FRR) and VPN reloaded unexpectedly when the interface went down and FRR was triggered.

Conditions: This symptom was observed on a router configured for FRR and VPN when running Cisco IOS Release 12.0(30)S.

Workaround: There is no workaround.

Further Problem Description: This symptom was only observed once and could not be reproduced. Use of VPN and many prefixes may contribute to this symptom.

- CSCeh05751

Symptoms: Hardware multicast may be disabled on an Engine 3 line card and the line card may reset.

Conditions: This symptom is observed when you scale BGP routes and load-balancing on a PE router that is configured for MVPN.

Workaround: There is no workaround.

- CSCeh06543

Symptoms: Ping packets that enter on ATM ISE line cards are punted to the RP and not reported by NetFlow. The raw cache entries and the aggregate cache entries do not appear for these ping packet. Even after increasing the cache timeout value, the entries do not appear.

Conditions: This symptom is observed on a Cisco 12000 series that is configured NetFlow and that has the **mpls traffic-eng tunnel** command enabled.

Workaround: There is no workaround.

- CSCeh09448

Symptoms: The MR-APS Active interfaces continue to be active until the deadman timer expires. This results in traffic loss even though another interface on another router could take over for this MR-APS group.

Conditions: This symptom is observed when the router is reloaded.

Workaround: To prevent traffic loss, do a manual switchover before the router is reloaded.

- CSCeh11537

Symptoms: The PIM neighbor ship on a VRF goes down, preventing traffic from flowing.

Conditions: This symptom is observed on a Cisco 12000 series that is configured for MVPN when you perform one of the following actions:

- You shut down a line card that is used by MVPN to punt control packets to the RP.
- You change the VRF name on the line card that is used by MVPN to punt control packets to the RP.

Workaround: If the symptom occurs because you shut down the line card, re-insert the line card to restore the PIM neighborhood. If the symptom occurs because you changed the VRF name on the line card, disable and re-enable the **mdt default group-address** command that is defined under the **ip vrf** command.

- CSCeh12675

Symptoms: Traffic may not fully converge after you have reloaded a line card with a scaled configuration or after an HA switchover.

Conditions: This symptom is observed on a Cisco 12416 that runs the c12kprp-p-mz image of a Cisco IOS interim release for Release 12.0(31)S and that is configured with dual PRPs and a scaled configuration.

Workaround: There is no workaround.

- CSCeh13895

Symptoms: When a 4-port OC-12 ATM ISE line card is deployed in the core between a P router and a PE router that performs decapsulation in a multicast VPN topology, packets with a size that is larger than 4447 bytes and that need fragmentation are not received by a CE router.

Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of Cisco IOS Release 12.0(28)S2 or a later 12.0S release.

Workaround: There is no workaround.

- CSCeh14063

Symptoms: MPLS Layer 3 VPN traffic cannot be forwarded from a main interface that is also used for Layer 3 VPN de-aggregation traffic and Layer 2 VPN traffic.

Conditions: This symptom is observed on Cisco 12000 series POS ISE line card that is configured for Frame Relay encapsulation when one of its subinterfaces is used for Layer 3 VPN de-aggregation and when a Frame Relay DLCI that is used for Layer 2 VPN traffic is configured on the same main interface.

Workaround: There is no workaround.

- CSCeh15364

Symptoms: On a router that is configured for multi-router APS, the APS interfaces remain in the Active/Inactive states. One of the interfaces is Active, while the other is Inactive. However, when the line card holding the APS protect interface is reloaded and the line card comes back up, both the Working and Protect interfaces end up in Active state.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S2. Not every protect line card reload causes the symptom occur. The symptom is readily observed when the reload of a Protect line card is accompanied by a simultaneously occurring Signal Fail/Signal Degrade (set/clear) event on the Working line card.

Workaround: There is no workaround to prevent the symptom from occurring. However, when both interfaces are in the Active state, a manual or forced APS switch may restore sanity to the APS states.

- CSCeh17756

Symptoms: The PIM assert mechanism may not function properly, causing PE routers to remove VRF subinterfaces from output interface lists, and, in turn, causing multicast traffic to be dropped.

Conditions: This symptom is observed when redundant PE routers and CE routers are located on one LAN segment and when the CE routers select different PE routers as their next hop.

Workaround: Change the configuration in such a way that all CE routers on one LAN segment select the same PE router as their next hop.

- CSCeh20201

Symptoms: Traffic entering a 1-port channelized OC-12/STM-4 (DS1/E1) ISE line card is dropped.

Conditions: This symptom is observed on a Cisco 12000 series when an MLP interface is moved from the 1-port channelized OC-12/STM-4 (DS1/E1) ISE line card to another line card.

Workaround: There is no workaround.

- CSCeh20219

Symptoms: The policer does not function for nxDs0 interfaces.

Conditions: This symptom is observed on a Cisco 12000 series that is configured with a 1-port channelized OC-12c/STM-4 (DS1/E1) ISE line card.

Workaround: There is no workaround.

- CSCeh20236

Symptoms: A Gigabit Ethernet port of an Engine 2 line card generates various error messages and tracebacks when it is brought up. This situation affects the traffic flow.

Conditions: This symptom is observed when the line card is installed in a Cisco 12816 that runs a Cisco IOS interim release for Release 12.0(31)S

Workaround: There is no workaround.

- CSCeh22267

Symptoms: A ping failure occurs between two SRP nodes.

Conditions: This symptom is observed when a Cisco 12000 series boots and is connected to another platform via the interface of a 1-port OC-192 DPT line card.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface of the 1-port OC-192 DPT line card.

- CSCeh22663

Symptoms: When a 4-port OC-12 ATM ISE line card is deployed in the network core between a P router and a PE router that functions as an encapsulation router in a multicast VPN topology, and when packets that need fragmentation are sent via the 4-port OC-12 ATM ISE line card from the PE router that performs encapsulation towards the P router, the packets do not arrive at the other end.

Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of a Cisco IOS interim release for Release 12.0(31)S.

Workaround: There is no workaround.

- CSCeh23047

Symptoms: After a manual SSO switchover, traffic in the tag switching-to-IP switching direction between an egress 1-port 10-Gigabit Ethernet Engine 4+ line card and an ingress 4-port Gigabit Ethernet ISE line card does not recover.

Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of Cisco IOS Release 12.0(31)S.

Workaround: Reload microcode onto the 4-port Gigabit Ethernet ISE line card.

- CSCeh25458

Symptoms: For line cards, the size of the memory that is used for boot records shows incorrect.

Conditions: This symptom is observed on a Cisco 12000 series.

Workaround: To show the correct memory size, enter the **show diag** command.

- CSCeh27734

Symptoms: For recursive routes with implicit null as the local label, the FIB may point to the rewrite of the parent prefix. However, this situation may not affect any functionality.

Conditions: This symptom is observed on a router that is configured for MPLS forwarding.

Workaround: Change the affected prefix to be non-recursive.

- CSCeh27783

Symptoms: A router crashes after you have manually configured 237 IPv6 tunnels.

Conditions: This symptom is observed on a Cisco platform that is configured for IPv6 when there are more than eight paths for one IPv6 prefix. The symptom is platform-independent and not release-specific.

Workaround: There is no workaround.

- CSCeh27890

Symptoms: A Engine 5 line card may crash just after the router has reloaded.

Conditions: This symptom is observed on a Cisco 12410 that runs a Cisco IOS interim release for Release 12.0(31)S.

Workaround: There is no workaround.

- CSCeh30324

Symptoms: An OIR of a CSC may cause all line cards in the router to enter the disabled state.

Conditions: The symptom is observed on a Cisco 12000 series that runs a Cisco IOS interim release for Release 12.0(31)S.

Workaround: There is no workaround.

- CSCeh30999

Symptoms: After you manually clear the tunnel between two PE routers or you reset one of the PE routers, more than two tunnels are created between the PE routers.

Conditions: This symptom is observed when multiple dynamic or static sessions are configured between two PE routers that are configured as L2TPv3 tunnel points.

Workaround: Reload both PE routers. If this not an option, there is no workaround.

- CSCeh31939

Symptoms: When a 1-port channelized OC-12/STM-4 (DS1/E1) ISE line card is configured for MVPN on MLP interfaces and you reload the router, the PIM VRF neighbor may not be established via a tunnel for some MLP interfaces.

Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of a Cisco IOS interim release for Release 12.0(31)S.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected MLP interfaces.

- CSCeh33574

Symptoms: An Engine 4 plus or Engine 5 line card does not come up.

Conditions: This symptom is observed on a Cisco 12000 series that runs a Cisco IOS interim release for Release 12.0(31)S when IPC timeout errors occur.

Workaround: There is no workaround.

- CSCeh34989

Symptoms: One of the following two symptoms may occur on a POS ISE egress line card:

- The interface may become stuck during transmission. The line protocol will continuously flap because the interface continues to receive keepalives but is not able to send any keepalives.
- The line card generates the following harmless error message:

```
%EE48-4-GULF_TX_SRAM_ERROR: ASIC GULF: TX bad packet header detected.
Details=0x4000
```

Conditions: These symptoms are observed on a Cisco 12000 series when an invalid packet is forwarded to an egress interface on an ISE line card.

Workaround: If the transmission on the interface is stuck, reload the line card by entering the **hw-module slot x reload** command.

- CSCeh35411

Symptoms: A 4-port OC-12 POS Engine 2 line card may crash repeatedly when the Cisco 12000 series in which the line card is installed comes up after a software-forced crash has occurred on the router.

Conditions: This symptom is observed on a Cisco 12000 series that runs the c12kprp-p-mz image of a Cisco IOS interim release for Release 12.0(31)S, that is configured with two RPS, and that is configured for SSO. The symptom is more likely to occur when the **ipv6 unicast-routing** command is enabled.

Workaround: To diminish the chance that the symptom occurs, disable the **ipv6 unicast-routing** command.

- CSCeh35422

Symptoms: A PRP switchover causes “%SYS-2-NOTQ” and “%SYS-2-LINKED” error messages and some tracebacks to be generated on a 1-port channelized OC-12c/STM-4 (DS1/E1) ISE line card, the serial interfaces of the line card flap, and eventually the line card resets.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S or Release 12.0(30)S, that is configured with two PRPs, and that has the redundancy mode set to SSO.

Workaround: There is no workaround.

- CSCeh37351

Symptoms: In a tag switching-to-IP switching scenario with an ISE ingress line card and an Engine 4 plus (E4+) egress line card, the following bad packets may be forwarded to the E4+ line card:

- tag2ip, with bad ip hdr cksum
- tag2ip, with ip->tl > L2
- tag2ip, with ip->tl < 20
- tag2ip, with ip options packets
- tag2ip, with ip options packets with bad ip hdr cksum
- tag2ip, with ip options packets with ip->tl > L2
- tag2ip, with ip options packets with ip->tl < 20

These bad packets cause packet corruption and an “TX192-3-PAM_PIM” error message on the E4+ line card and may even cause the E4+ line card to reset.

Conditions: This symptom is observed on a Cisco 12000 series.

Workaround: There is no workaround.

Further Problem Description: The fix for this caveat enables the ISE line card to drop the above-mentioned bad packets.

- CSCeh39850

Symptoms: When an attachment circuit is configured for ATOM pseudowire redundancy, an MPLS core network failure on the primary pseudowire may not cause a switchover to the redundant (or backup) pseudowire.

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.2(27)SBA and on a Cisco 12000 series that runs a Cisco IOS interim release for Release 12.0(31)S.

Workaround: There is no workaround.

- CSCeh40556

Symptoms: Links flap on a 1-port channelized OC-12/STM-4 (DS1/E1) ISE line card after an RP switchover has occurred.

Conditions: This symptom is observed on a Cisco 12000 series that has two PRPs and that runs Cisco IOS Release 12.0(31)S.

Workaround: There is no workaround.

- CSCeh42465

Symptoms: An Engine 3 line card sends unlabeled traffic after it has been toggled from explicit routing to default routing. The symptom is related to the handling of a default-route on an Engine 3 ingress line card that functions in an IP-to-MPLS path.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(30)S1 or any other image that includes the fix for caveat CSCsa64782, which is a preliminary requisite for default-route handling on an Engine 3 line card. The symptom occurs in the following scenario:

1. You configure BGP to advertise the target address, so the target address is directly known in the routing table.
2. You remove the advertisement from BGP and return to default routing, with the same source for the next hop as the platform that was the BGP next hop.
3. You enter the **clear ip route network** command, with the address of the BGP next hop for the *network* argument.

After the transition from non-default routing to default routing, entering the **clear ip route network** command, with the address of the next hop for the *network* argument, causes an inconsistency, and traffic is forwarded as unlabeled.

Workaround: To restore proper operation, enter the **clear ip route 0.0.0.0** command.

- CSCeh42812

Symptoms: An RP switchover may cause CEF inconsistency on line cards.

Conditions: This symptom is observed on a Cisco 12000 series that runs a Cisco IOS interim release for Release 12.0(31)S and that has two PRPs that function in RPR+ redundancy mode.

Workaround: If all line cards are affected, enter the **clear cef linecard** command. If a specific line card is affected, enter the **clear cef linecard slot-number** command. Enter these command from a console that is attached to the RP or RRP.

- CSCeh49881

Symptoms: In a tag switching-to-IP switching scenario with an ISE ingress line card and an Engine 4 plus (E4+) egress line card, the following bad packets may be forwarded to the E4+ line card:

- tag2ip, with bad ip hdr cksum
- tag2ip, with ip->tl > L2
- tag2ip, with ip->tl < 20
- tag2ip, with ip options packets
- tag2ip, with ip options packets with bad ip hdr cksum
- tag2ip, with ip options packets with ip->tl > L2
- tag2ip, with ip options packets with ip->tl < 20

These bad packets cause packet corruption and an “TX192-3-PAM_PIM” error message on the E4+ line card and may even cause the E4+ line card to reset.

Conditions: This symptom is observed on a Cisco 12000 series.

Workaround: There is no workaround.

Further Problem Description: The fix for this caveat enables the ISE line card to drop the above-mentioned bad packets.

- CSCeh51720

Symptoms: When the router is configured with a new area, the links that are configured for TE are not flooded in the new area.

Conditions: This symptom is observed when you configure an area by entering the **mpls traffic-eng area number** command as part of the router OSPF configuration.

Workaround: There is no workaround.

- CSCeh53373

Symptoms: A TE tunnel does not come up.

Conditions: This symptom is observed in an MPLS TE interarea configuration.

Workaround: There is no workaround.

- CSCeh57695

Symptoms: A PE router that is configured for MPLS VPN—Carrier Supporting Carrier drops decapsulation traffic in the direction of a CE router. Encapsulation traffic works fine and is not affected.

Conditions: This symptom is observed when MPLS VPN—Carrier Supporting Carrier is configured with Label Distribution Protocol (LDP) as the protocol between the PE router and a CE router. In some circumstances such as a BGP peer flap or a route flap, LDP may free the local label that is allocated by BGP while BGP still uses the label. The same label may be allocated later for a different prefix, causing multiple prefixes to use the same local label, and, in turn, causing connectivity for the affected prefixes to fail.

Workaround: There is no workaround.

- CSCeh59452

Symptoms: An RP switchover may cause a 6-port channelized T3 Engine 0 line card to fail.

Conditions: This symptom is observed on a Cisco 12000 series that runs a Cisco IOS interim release for Release 12.0(31)S, that has two PRPs, and that functions in RPR+ redundancy mode.

Workaround: There is no workaround.

- CSCin65637

Symptoms: Latency is higher when priority queueing is configured for an interface of a 2-port Packet-over-SONET OC-3c/STM-1 port adapter (PA-POS-2OC3). Latency is higher even for priority packets.

Conditions: This symptom is observed when the data rate exceeds the OC-3 line rate and may occur on all types of VIPS on a Cisco 7500 series and on a Cisco 7200 series that is configured with an NPE-300, NPE-400, or NSE-1. The symptom does not occur on a Cisco 7200 series that is configured with an NPE-G1.

Workaround: To prevent the data rate from exceeding the OC-3 line rate, configure traffic shaping. This also brings the latency for priority packet to tolerable limits.

- CSCin67253

Symptoms: A Cisco 7500 series may stop forwarding traffic via an Any Transport over Multiprotocol Label Switching (AToM) virtual circuit (VC) that is configured on an 8-port multichannel T1/E1 PRI port adapter (PA-MC-8TE1+).

Conditions: This symptom is observed on a Cisco 7500 series that has a PA-MC-8TE1+ that is configured for Frame Relay over Multiprotocol Label Switching (FRoMPLS) or Frame Relay/ATM/Ethernet interworking when you perform an online insertion and removal (OIR) of the Versatile Interface Processor (VIP) in which the PA-MC-8TE1+ is installed.

Workaround: Remove and reconfigure the affected AToM VC.

- CSCin75746

Symptoms: When you perform an OIR of a PA-MC-8TE1 port adapter or you reload microcode onto the line card, the line card may generate the following error message and may stop forwarding traffic:

AC Switching: VIP Xmit failed: DLCI 426 context missing

Conditions: This symptom is observed on a Cisco 7500 series.

Workaround: There is no workaround. To re-enable the line card, enter the **tx-queue-limit** command on the affected interface of the line card.

- CSCin79899

Symptoms: When error recovery is performed on a 3-port Gigabit Ethernet (GE) line card that has port 0 in the shutdown state, the 3-port GE line card stop passing traffic on all ports.

Conditions: This symptom is observed on a Cisco 12410 that runs Cisco IOS Release 12.0(23)S or a later release and that is configured with an Engine 2 3-port line card.

Workaround: Reload the 3-port GE line card and leave port 0 in the up/down state.

- CSCin80743

Symptoms: Configurations of interfaces on a legacy interface processor such as an EIP or an FSIP on a Cisco 7500 series go down after a redundancy-forced switchover.

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(28)S or a later release or Release 12.2(25)S that is configured for SSO or RPR+.

Workaround: Manually reconfigure the interfaces.

- CSCin81933

Symptoms: At a cold temperature, a Cisco 7200 series does not boot with a PA-A3-8T1IMA or PA-A3-8E1IMA port adapter and generates a watchdog timeout error.

Conditions: This symptom is observed on a Cisco 7200 series that is configured with an NPE-300 or NPE-400 and an IMA port adapter.

Workaround: There is no workaround.

- CSCin82862

Symptoms: Multicast traffic is not switched from a multilink interface on a Cisco 7500 series that is configured for distributed multilink PPP (MLP).

Conditions: This symptom is observed when the router is reloaded or when the multilink interface flaps.

Workaround: Enter the **clear ip mds linecard *** command on the Route/Switch Processor (RSP).

- CSCin83445

Symptoms: Incoming multicast traffic on a distributed MLP link is process-switched.

Conditions: This symptom is observed on a Cisco 7500 series that is configured for distributed MLP after the router has been reloaded.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected multilink interface.

- CSCin84124

Symptoms: After performing a Fast Software Upgrade (FSU), none of the interfaces of the active RSP come up.

Conditions: This symptom is observed on a Cisco 7500 series after you have performed a FSU to Cisco IOS Release 12.2(25)S or Cisco IOS Release 12.0(30)S and after an SSO switchover has occurred.

Workaround: After the FSU, enter the **microcode reload** command.

- CSCin86885

Symptoms: A VIP6-80 in which a PA-MC-STM-1SMI is installed may crash.

Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS interim release for Release 12.0(31)S after link flaps occur on the PA-MC-STM-1SMI that has QOS configured on its serial interfaces.

Workaround: There is no workaround.

- CSCin87776

Symptoms: Multilink bundles on a Cisco 7500 series may process-switch traffic instead of using dCEF, causing the CPU usage of the RSP to increase sharply and a CPU hog condition to occur.

Conditions: This symptom is observed when an RPR+ switchover occurs on a Cisco 7500 series that is configured for HA. (The switchover causes an MLP to flap.) However, the symptom may also occur on a Cisco 7500 series that has a single RP (so, without a switchover) when an MLP link flaps.

Workaround: There is no workaround. Note that the symptom does not occur when SSO is configured because the MLP state is maintained.

- CSCin88026

Symptoms: A VIP that is configured for Link Fragmentation and Interleaving may crash during the “vip_mlp_process_reassemble” process.

Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS interim release for Release 12.0(31)S when links flaps occur on the port adapter that is installed in the VIP while traffic is being processed.

Workaround: There is no workaround.

- CSCin88273

Symptoms: After an RPR+ or SSO switchover occurs, an MLP sequence number mismatch may occur, a ping between back-to-back interfaces may not go through, and the routing protocol through this link may go down.

Conditions: This symptom is observed on a Cisco 7500 series that is configured for dMLP and RPR+ or SSO.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the multilink interface of the Cisco 7500 series.

- CSCin88303

Symptoms: The line protocol of unchannelized interfaces on a PA-MC-2T3+ port adaptor remains down although the link is up.

Conditions: This is observed when you change from the channelized mode to the unchannelized mode by entering the **no channelized** command on the T3 controller of the PA-MC-2T3+ port adaptor.

Workaround: There is no workaround.

- CSCin88356

Symptoms: The output of the **show interfaces serial number** command does not show the total output packet drops.

Conditions: This symptom is observed when you apply a service policy on an interface that is configured for CEF.

Workaround: Enter the **show policy map interface interface-name** command to see the total output packet drops.

- CSCin88417
Symptoms: Transmit accumulator loss may occur for MLP interfaces after you have performed an OIR of a VIP. When the transmit accumulator value goes to zero, MLP may stop forwarding or packets may be switched by dCEF.
Conditions: This symptom is observed after you have performed an OIR of a VIP while traffic is running on MLP bundles.
Workaround: Reload the VIP again and ensure that no traffic leaves from the MLP bundles immediately after the VIP comes up.
- CSCin89330
Symptoms: Distributed MFR does not function, that is, a ping on a distributed MFR interface fails.
Conditions: This symptom is observed on a Cisco 7500 series that has a distributed MFR interface.
Workaround: There is no workaround.
- CSCsa42857
Symptoms: A duplex configuration (half/full) is not saved to NVRAM. This situation causes the default configuration (half duplex) to be used after the router reloads.
Conditions: This symptom is observed on a PA-2FE port adapter that is installed in a Cisco 7200 series that runs Cisco IOS Release 12.0(28)S1.
Workaround: There is no workaround.
- CSCsa46154
Symptoms: A Route Processor (RP) failover occurs.
Conditions: This symptom occurs when you enter the **show route-map** command in one session and remove several route maps in rapid succession in another session.
Workaround: Do not enter the **show route-map** command when you remove route maps in a concurrent vty session.
- CSCsa46699
Symptoms: A Cisco 7200 series may crash because of a bus error when you remove a subinterface or when you remove a service policy from an interface.
Conditions: This symptom is observed when a hierarchical policy map is configured, when the policy map has a police action in the child only, and when the policy map is attached to two interfaces. When the service policy is removed from one of the interfaces, the router may crash.
Workaround: Configure the same policy map with a different name on each interface.
- CSCsa46887
Symptoms: A router builds an Echo Reply that is invalid and may be misunderstood.
Conditions: This symptom is observed on a router that is configured for LSPV when the router receives an Echo Request with a Pad TLV that has a value of "Copy Pad TLV to reply." The Echo Reply that the router builds includes residual data from previously received packets instead of the pad pattern that was received.
Workaround: There is no workaround.
- CSCsa47020
Symptoms: When Multilink Frame Relay (FRF.16) is configured on two bundled serial links and when the traffic rate is above 2 Mbps, packet loss occurs.

Conditions: This symptom is observed on a Cisco Catalyst 6500 series and a Cisco 7500 series when you send a 64-byte Ethernet frame. The symptom does not occur when the frame size is 512 bytes or more.

Workaround: There is no workaround.

- CSCsa49740

Symptoms: Packets are punted to the GRP at a rate of 5000 pps, causing the CPU utilization of the CPU to reach more than 50 percent.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(26)S3 when a 4-port Packet-over-SONET OC-48c Engine 4 plus line card (4OC48E/POS-SR-SC=) receives TCP packets with destination 0.0.0.0.

Workaround: There is no workaround.

- CSCsa52944

Symptoms: The peak information rate (PIR) receives a random value when a 2-rate 3-color color-aware MQC policing policy is configured. When you save the configuration and reload the router, the PIR value is changed into a huge value.

Conditions: These symptoms are observed on a Cisco 12000 series that runs an interim release for Cisco IOS Release 12.0(31)S.

Workaround: There is no workaround.

Further Problem Description: If PIR has a huge value, it is likely that incoming traffic never violates the policy.

- CSCsa53001

Symptoms: A VIP6-80 in which a PA-MC-STM-1SMI is installed crashes.

Conditions: This symptom is observed on a Cisco 7500 series that runs a Cisco IOS interim release for Release 12.0(31)S after link flaps occur on the PA-MC-STM-1SMI that has QoS configured its serial interfaces.

Workaround: There is no workaround.

- CSCsa53685

Symptoms: Incorrect VC12 defect information may be generated on a Cisco 7500 series that is configured with a PA-MC-STM-1.

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(28)S1.

Workaround: There is no workaround.

- CSCsa54891

Symptoms: Under normal operation, an Engine 6 line card may reset with the following error messages and tracebacks:

```
%TX192-3-CPUIF: Error=0x10
rd 0x73 base 0x73 hdr 0x75 last 0x75 wr 0x75
insert 0x0 back 0x0 len 0x2474 cnt 0x0
-Traceback= 40D89758 405A9008 405EC67C 406D5E7C 406D64F8 400FC020
%TX192-3-CPUIF_ERR: FIFO RAM3 Parity Error.
-Traceback= 40D89808 405A9008 405EC67C 406D5E7C 406D64F8 400FC020
%GSR-3-INTPROC: Process Traceback= 400FFD20 400FCAA0 40010F6C
-Traceback= 404EFBCC 406D6760 400FC020
%FABRIC-3-ERR_HANDLE: Due to FIA HALT error, reconfigure FIA on slot 9
```

Conditions: This symptom is observed on a Cisco 12000 series when false RAM parity errors occur.

Workaround: There is no workaround.

Further Problem Description: The fix for this caveat determines whether the RAM parity errors are real or false.

- CSCsa55048

Symptoms: The content of the CEF table may be incorrect, causing less than optimal traffic conditions.

Conditions: This symptom is observed when a static route is configured in one VRF and exported with an export map into another VRF and when this static route is added on two separate PE routers.

Workaround: Do not configure the static router on both PE routers. If this is not an option, there is no workaround.

- CSCsa56032

Symptoms: Packets are dropped on a CE router in an MPLS VPN network.

Conditions: This symptom is observed when a connected Cisco 10720 that functions as the PE router shows a “bad ip checksum” counter in the output of the **show hardware pxf cpu statistics interface interface detail** command for its Parallel Express Forwarding engine. The PE router has the **mpls ldp explicit-null** command configured and has both input and output service policies.

Workaround: Remove the **mpls ldp explicit-null** command from the PE router.

- CSCsa56142

Symptoms: Entering the **no export map** VRF configuration mode command has no effect.

Conditions: This symptom is observed on a Cisco router that is configured for RPR+ or SSO when the you take the following steps:

1. You enter the **no export map** VRF configuration mode command on the active RP.
2. You enter the **write memory** command.
3. You initiate an RPR+ or SSO switchover.

After these steps, the export map is still configured on the new active RP, while it should no longer be present.

Workaround: Manually remove the export map from the new active RP.

- CSCsa56415

Symptoms: A router may pause indefinitely or reload unexpectedly.

Conditions: This symptom is observed while deleting or recreating policing access control lists (ACLs) or shaping ACLs via a script.

Workaround: Update the access control list (ACL) rather than delete it.

- CSCsa59002

Symptoms: IP fragments with a User Datagram Protocol (UDP) protocol identifier may be improperly denied on an Engine 3 line card that has an outbound access control list (ACL) that denies specific UDP ports.

Conditions: This symptom is observed only for outbound ACLs on an Engine 3 line card on a Cisco 12000 series. The following is an example of an ACL statement for which the symptom may occur:

```
access-list 100 deny udp any any eq 0 <<< this line may accidently deny IP fragments
for UDP access-list 100 permit ip any any
```

Workaround: Use the following ACL instead of the above-mentioned example:


```
access-list 101 permit udp any any fragments
access-list 101 deny udp any any eq 0
access-list 101 permit ip any any
```

- CSCsa61687

Symptoms: A router crashes when you enter the **show sss memory** command.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S.

Workaround: There is no workaround.

- CSCsa64782

Symptoms: When an ingress ISE line card is used with a default route that iBGP learns over a MPLS core, the following two symptoms may occur:

- The output of the **show controllers tofab alpha mip stat | i MTU** command may show traffic drops.
- Traffic is incorrectly sent as “unlabeled” over the MPLS core.

Conditions: These symptoms are observed on a Cisco 12000 series when the traffic path follows a recursive default route and when recursive load sharing occurs.

Workaround: Prevent recursive load sharing by changing the IGP metrics.

- CSCsa66198

Symptoms: A Dynamic Packet Transport (DPT) ISE line card crashes when you attach a service policy.

Conditions: This symptom is observed on a Cisco 12000 series.

Workaround: There is no workaround. You cannot use QoS on the DPT ISE line card.

- CSCsa68240

Symptoms: Interfaces of an Engine 4 POS line card may not enter the up/up state.

Conditions: This symptom is observed on a Cisco 12000 series after you have changed the Cisco IOS software image.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected POS interfaces to enable them to enter the up/up state.

- CSCsa68301

Symptoms: Inter-MVPN traffic does not function on an Engine 4+ line card.

Conditions: This symptom is observed on a Cisco 12000 series and may occur with any Engine 4+ line card.

Workaround: There is no workaround.

- CSCsa68616

Symptoms: An IPC failure occurs and an OC-12 line card that is configured for Frame Relay over MPLS resets.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(27)S1.

Workaround: There is no workaround.

Further Problem Description: The IPC failure and the line card reset occur after a depletion of the elements in the FrFab 608 byte queue for the line card. Consecutive outputs of the **show controllers slot-number frfab queue** command show a consistent and rapid leak of these buffers.

- CSCsa70274

Symptoms: A Cisco router may crash during an LSP traceroute when a transit router responds with a downstream map TLV that contains a multipath length field that is set to 0, 1, 2, or 3.

Conditions: This symptom is observed during testing of the Cisco LSP ping draft version 3 in a network that uses a later version of the LSP ping draft.

The implementation of draft version 3 does not handle the multipath length field settings correctly. In draft version 3 and earlier drafts, there is an ambiguity on whether or not the multipath length field includes the four bytes comprising of the hash-key type, depth limit, and multipath length fields. As such, all implementations of the draft version 3 encode the length as four bytes and reply with a multipath length of four bytes.

When an LSP traceroute is invoked and a transit router replies with a downstream map TLV that contains a multipath length field that is set to a length shorter than four bytes, existing implementations handle this situation incorrectly and cause memory packet memory to become corrupted during the subsequent attempt to build an MPLS echo request packet. This situation eventually causes the router to crash.

Workaround: If LSP traceroute implementations exist on a transit router that cause the transit router to reply with a multipath length that is set to a value other than four, avoid using an LSP traceroute.

Note, however, that the implementations of Cisco LSP ping draft version 3 do not reply with multipath lengths that can cause this crash.

- CSCsa75375

Symptoms: You cannot configure the **speed** command on Ethernet interfaces.

Conditions: This symptom is observed on a Cisco 10720.

Workaround: There is no workaround.

- CSCuk55066

Symptoms: When you attach a policy to an interface of an Engine 3 4-port Gigabit Ethernet line card, the following error message is generated:

```
% Ignoring non "match vlan/dlci" entries in class <class-name> in policy <policy name>
on <interface-name>.
```

However, the policy remains attached to the interface.

Conditions: This symptom is observed on a Cisco 12000 series that runs a Cisco IOS release later than interim Release 12.0(29.4)S. The symptom occurs with all kinds of policies and with different class maps.

Workaround: There is no workaround.

- CSCuk55561

Symptoms: A compact flash (CF) disk that is formatted in Cisco IOS-XR software does not mount on a platform that runs Cisco IOS software. The compact flash disk is successfully formatted from Cisco IOS-XR software, however, the **show compactflash: filesys** command reports the wrong device format.

Conditions: This symptom is observed when a compact flash disk that is formatted by Cisco IOS-XR software is used on a platform that runs Cisco IOS software.

Workaround: Format the disk using Cisco IOS.

- CSCuk55653
Symptoms: QoS may not function on a Cisco 12000 series ATM ISE line card.
Conditions: This symptom is observed on a Cisco 12000 series that runs an interim release of Cisco IOS Release 12.0(31)S when you apply the same policy on at least two VCs and when the policy consists of at least two classes: one with a police action and two without police actions.
Workaround: Remove and reconfiguration the class map.
- CSCuk55758
Symptoms: On Cisco 7500 series routers and Cisco Catalyst 6500 series switches with MSFC cards, distributed CEF does not automatically become enabled after issuing an **ip routing** command.
The output from the **show cef state** command shows that the distributed CEF state is “dCEF disabled/not running”, and the packet forwarding performance is very poor.
Conditions: This symptom is observed only in a Cisco IOS interim release for Cisco IOS Release 12.0(30)S and an interim release for Release 12.2S.
Workaround: Enable distributed CEF by using the **ip cef distributed** command.
- CSCuk55912
Symptoms: You cannot ping from an Engine 2 OC-48 SRP interface, preventing a topology from being received.
Conditions: This symptom is observed after you have booted a Cisco 12000 series and “WRAPPING_PROCESS_LOCKED” error messages have been generated.
Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface.
- CSCuk56024
Symptoms: 6PE traffic is dropped on a PE router.
Conditions: This symptom is observed when an IPv6 prefix is first learned by an OSPF IGP on a 6PE router but then no longer received by OSPF but iBGP on the 6PE router. The label information is properly updated in the RIB but not in the FIB.
Workaround: Clear the route to restore proper forwarding.
- CSCuk56335
Symptoms: You cannot forward traffic over an Engine 2 OC-48 SRP interface and the following error message is generated:

```
IDBINDEX_SYNC-3-IDBINDEX_ENTRY_SET FIB-4-FIBIDB: Missing cef idb for SRP3/0 during address change
```


Conditions: This symptom is observed after you have booted a Cisco 12000 series.
Workaround: There is no workaround.

TCP/IP Host-Mode Services

- CSCeg20351
Symptoms: An RR is unable to negotiate the optimal MSS with their MP-BGP neighbors.
Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.0(28)S1, that functions as an RR, and that has Path MTU Discovery (PMTUD) enabled. The symptom may also occur in other releases.
Workaround: There is no workaround.

Wide-Area Networking

- CSCea30197

Symptoms: When the *keep-exchanges* argument in the **frame-relay lmi-n391dte** *keep-exchanges* command has a value that is lower than 3, Frame Relay Autosensing does not function.

Conditions: This symptom is observed on a Cisco 7500 series and Cisco 7600 series but may be platform-independent.

Workaround: Ensure that the value of the *keep-exchanges* argument is not lower than 3.
- CSCef71011

Caveat: Pings fail when Translational Bridging and ATM DXI encapsulation are configured.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0S, Release 12.2S, or a release that is based on Release 12.2S.

Workaround: Do not configure ATM DXI encapsulation. Rather, configure HDLC, PPP, or Frame Relay encapsulation.
- CSCeg53851

Symptoms: IP routes are not updated across an ISDN link.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0S or interim Release 12.3(12.8).

Workaround: There is no workaround.
- CSCeg88174

Symptoms: Drops occur in a class in which the throughput does not oversubscribe the allocated bandwidth for the class.

Conditions: This symptom is observed when multilink Frame Relay is configured along with generic traffic shaping or Frame Relay traffic shaping and when several class maps are configured.

When one class map starts dropping packets because the throughput is greater than the allocated bandwidth (which is normal behavior), drops may also occur in another class map even though this class map is not oversubscribed. The root cause of this symptom is that the bundle is oversubscribed and tx rings are building up, causing excessive misordering that the receiver cannot handle.

Workaround: Configure a fancy queue on the bundle interface through which the traffic is sent.
- CSCeg88737

Symptoms: A Cisco 7200 series may crash because of memory corruption.

Conditions: This symptom is observed when the router has an input QoS configuration on an MFR interface.

Workaround: There is no workaround.
- CSCsa49019

Symptoms: A memory leak may occur in the “Multilink Events” process, which can be seen in the output of the **show memory summary** command:

0x60BC47D0	0000000024	0000000157	0000003768	MLP bundle name
0x60BC47D0	0000000028	0000000003	0000000084	MLP bundle name
0x60BC47D0	0000000044	0000000001	0000000044	MLP bundle name
0x60BC47D0	0000000048	0000000001	0000000048	MLP bundle name
0x60BC47D0	0000000060	0000000001	0000000060	MLP bundle name
0x60BC47D0	0000000064	0000000013	0000000832	MLP bundle name

```

0x60BC47D0 0000000068 0000000008 0000000544    MLP bundle name
0x60BC47D0 0000000072 0000000001 0000000072    MLP bundle name
0x60BC47D0 0000000076 0000000001 0000000076    MLP bundle name
0x60BC47D0 0000000088 0000000018 0000001584    MLP bundle name

```

Conditions: This symptom is observed when two interfaces are configured in the same multilink group or are bound to the same dialer profile.

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.0(30)S5

Cisco IOS Release 12.0(30)S5 is a rebuild of Cisco IOS Release 12.0(30)S. The caveats listed in this section are resolved in Cisco IOS Release 12.0(30)S5 but may be open in previous Cisco IOS releases. This section describes only severity 1, severity 2, and select severity 3 caveats.

Basic System Services

- CSCsb98906

Symptoms: A memory leak may occur in the “BGP Router” process.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(26)S6, that is configured for BGP, and that has the **bgp regexp deterministic** command enabled.

Workaround: Disable the **bgp regexp deterministic** command.

Interfaces and Bridging

- CSCsa46510

Symptoms: When you enter the **microcode reload** command, an error message similar to the following and a traceback may be generated:

```

RSP-3-RESTART: interface Serial3/0/1/4:0, not transmitting -Traceback= 404436B4
4044DE10

```

Conditions: This symptom is observed on a Cisco 7500 that is configured with an E1, T1, E3, or T3 port adapter.

Workaround: There is no workaround.

- CSCsc17534

Symptoms: Unicast packets are not CEF-switched on a VIP but are fast-switched on the RP.

Conditions: This symptom is observed on a Cisco router that has a VIP only when the ingress interface is an ISL subinterface.

Workaround: There is no workaround.

- CSCsc69537

Symptoms: A Cisco 12000 series may report incorrect ifIndex values in the NetFlow Data Export (NDE) packets that are sent from a Gigabit Ethernet (GE) ISE line card. Flows that arrive via VLAN subinterfaces may be reported as zero with the SNMP ifIndex or as the ifIndex of the physical GE interface.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(30)S3 or a later release after you have reloaded the GE line card.

Workaround: There is no workaround. When the symptom has occurred, re-apply the configuration of the subinterfaces.

- CSCsc71286

Symptoms: The throughput is far below what you would expect on an MFR bundle that is configured on a 8-port multichannel T1/E1 PRI port adapter (PA-MC-8TE1+).

Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.0(31)S2 when the MFR bundle has four T1 links, three of which are shut down. When you generate 2.5 Mbps of traffic to congest the one active link, a throughput of about 37 kbps to 59 kbps is observed. You would expect a throughput of about 1.5 Mbps.

Workaround: There is no workaround. The symptom does not occur in Release 12.3.

IP Routing Protocols

- CSCec12299

Devices running Cisco IOS versions 12.0S, 12.2, 12.3 or 12.4 and configured for Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) or VPN Routing and Forwarding Lite (VRF Lite) and using Border Gateway Protocol (BGP) between Customer Edge (CE) and Provider Edge (PE) devices may permit information to propagate between VPNs.

Workarounds are available to help mitigate this vulnerability.

This issue is triggered by a logic error when processing extended communities on the PE device.

This issue cannot be deterministically exploited by an attacker.

Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080924-vpn.shtml>.

- CSCei16615

Symptoms: A neighbor reloads when you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on an interface of an LSP router that functions as a tunnel headend.

Conditions: This symptom is observed when the following events occur:

- The tunnel headend sends a Path via RSVP to the neighbor but the Resv message is delayed.
- There is only one Path to the neighbor for the session.
- At the neighbor, the cleanup timer for the Path expires before the Resv message arrives, causing the session to be terminated.

Workaround: There is no workaround.

- CSCsb09852

Symptoms: The number of networks in the BGP table and the number of attributes increases, and a slower convergence may occur for members of a BGP update group.

Conditions: This symptom is observed on a Cisco router when the members of a BGP update group go out of synchronization with each other in such a way that they have different table versions, preventing the BGP Scanner from freeing networks that do not have a path.

To check if the members of the BGP update group are in synchronization with each other, enter the **show ip bgp update-group summary** command and look at the table version for each member. If they have the same table version, they are in synchronization with each other; if they do not, they are out of synchronization with each other.

Workaround: To enable the members of the BGP update group to synchronize with each other, enter the **clear ip bgp * soft out** command. Doing so does not bounce the sessions but forces BGP to re-advertise all prefixes to each member.

- CSCsb36755

Symptoms: When BGP receives an update that has a worse metric route than the previously received route for equal-cost multipath, the BGP table is updated correctly but the routing table is not, preventing the old path from being deleted from the routing table.

Conditions: This symptom is observed on a Cisco router that is configured for BGP multipath.

Workaround: Enter the **clear ip route network** command.

- CSCsb74708

Symptoms: An OSPF sham link may not form an adjacency.

Conditions: This symptom is observed when there is an interface in the global route table that has an IP address that matches the IP address of the OSPF sham link neighbor.

Workaround: Reconfigure the routers so that the IP address of the OSPF sham link neighbor does not match any IP addresses of interfaces in the global route table.

Alternate Workaround: Shut down the interface or change the IP address of the interface in the global route table.

- CSCsb79749

Symptoms: The output of the **show memory summary** command may contain garbled characters in the “What” column.

Conditions: This symptom is observed when you configure OSPF with at least one network, and then unconfigure it.

Workaround: There is no workaround.

- CSCsc59089

Symptoms: BGP does not advertise all routes to a peer that sends a route-refresh request.

Conditions: This symptom is observed under the following conditions:

- The router is in the process of converging all of its peers and has updates ready in the output queue for the peer.
- The peer sends a route-refresh request to the router. This may occur when the **clear ip bgp * soft in** command is entered on the peer or when a VRF is added to the peer.
- The router processes the route-refresh request from the peer while the router still has updates in the output queue for the peer.

In this situation, all of prefixes that are advertised by the unsent updates in the output queue for the peer are lost.

Workaround: There is no workaround. When the symptom has occurred, enter the **clear ip bgp * soft out** command on the router to force the router to send all updates to its peers.

- CSCsc75426

Symptoms: A router that is configured for BGP and that has the **ip policy-list** command enabled may unexpectedly reload because of a bus error or SegV exception.

Conditions: This symptom is observed when BGP attempts to send an update with a “bad” attribute.

Workaround: There is no workaround.

ISO CLNS

- CSCsb34032

Symptoms: A router may reload unexpectedly when you remove the IS-IS configuration at the interface or router level.

Conditions: This symptom is observed on a Cisco router when the following conditions are present:

- The router is HA-capable.
- The **isis protocol shutdown** interface configuration command is enabled on the interface.
- You enter an interface configuration command that enables IS-IS such as an **isis** command, a **clns** command, or the **ipv6 router isis** before you enter the a router configuration command such as the **net** command.

When you now remove the IS-IS configuration at the interface or router level, the router may reload.

Workaround: Remove the **isis protocol shutdown** interface configuration command before you remove IS-IS from the interface or router level.

- CSCsc63871

Symptoms: When IS-IS and CLNS are configured, a router may enter a state in which only one adjacency is shown in the output of the **show clns interface** command, even though the **show clns neighbors** command may correctly display all the neighbors that are connected to the interface.

When this situation occurs and any one of the neighbors on the segment goes down, all routing updates may be lost. The single adjacency is torn down and despite the fact that the output of the **show clns neighbors** command still shows the neighbors, routing stops because there are no adjacencies.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(18)S1 or Release 12.3(9b) when an adjacency goes down while it is still in the INIT state. The symptom occurs because the adjacency counter is incorrectly decremented. The symptom may also occur in other releases.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface that reports only one adjacency.

Alternate Workaround: Enter the **clear clns neighbors** command on the affected router.

Miscellaneous

- CSCeb05456

Symptoms: A Cisco platform may reset its RP when two simultaneous **write memory** commands from two different vty connections are executed, and messages similar to the following may appear in the crashinfo file:

```
validblock_diagnose, code = 10
current memory block, bp = 0x48FCC7D8, memory pool type is Processor data check, ptr
= 0x48FCC808
next memory block, bp = 0x491AC060, memory pool type is Processor data check, ptr =
0x491AC090
previous memory block, bp = 0x48FCBBE8, memory pool type is Processor data check, ptr
= 0x48FCBC18
```

The symptom is intermittent and is related to the way NVRAM is accessed.

Conditions: This symptom is observed on a Catalyst 6000 series Supervisor Engine 720 that runs Cisco IOS Release 12.2(18)SXD but is platform- and release-independent.

Workaround: Set the boot configuration to non-NVRAM media such as a disk or bootflash by entering the following commands:

```
boot config disk0:
filename
nvbypass
```

- CSCeb06452

Symptoms: When multicast IP version 6 (IPv6) Cisco Express Forwarding (CEF) is enabled, packets that are forwarded and that greater than or equal to 232 bytes may be corrupted.

Conditions: This symptom is observed on a Cisco platform that is configured for multicast CEF.

Workaround: Do not use CEF. Rather, use process-switching.

- CSCed29863

Symptoms: TU alarms and some SONET statistics are not reported correctly.

Conditions: This symptom is observed on a Cisco 10000 series that is configured with a 4-port channelized STM-1/OC-3 line card.

Workaround: There is no workaround.

Further Problem Description: A loss of multiframe (LOMF) alarm is reported on the E1 level instead of the TU level. Some SONET statistics are not reported correctly for multi-port cards. For example, the statistics for port 4 are displayed for ports 1, 2 and 3.

- CSCee22454

Symptoms: If a packet comes in through an interface on which RPF is enabled and the RPF check lookup results in a default prefix which has the Leaf NULL bit set, the packet is dropped even though the Leaf pointers are valid.

You can see the RPF drops by entering the **show hardware pxf interface** *interface-number* **detail | inc RPF** command.

Conditions: This symptom is observed when a Cisco 10000 series has two paths in the routing table installed for the default prefix 0.0.0.0/0 and when the default prefix is a recursive route. This situation causes the Leaf NULL bit to be set. The Leaf NULL bit is used only by the RPF check. If a packet arrives on an RPF-enabled interface and the RPF check lookup results in the default prefix, the packet is dropped because the Leaf NULL bit is set.

Workaround: Avoid loadsharing, that is, ensure that there is only one path.

- CSCef12139

Symptoms: Tracebacks are generated for an 8-port Fast Ethernet half-height line card when the router boots.

Conditions: This symptom is observed on a Cisco 10000 series.

Workaround: There is no workaround.

- CSCef98037

Symptoms: Incoming multicast traffic that is forwarded via the main interface of a Cisco 10000 series is dropped.

Conditions: This symptom is observed on a Cisco 10000 series that has a Gigabit Ethernet main interface that is configured with a number of VRF-enabled VLAN subinterfaces.

Workaround: Remove the VRFs from the VLAN subinterfaces.

- CSCeg07617

Symptoms: The following error message and spurious memory access may be generated on a Cisco 7500 series or Cisco 7600 series that is configured for dMLFR.

```
%ALIGN-3-SPURIOUS: Spurious memory access made at 0x418FC0E0 reading 0x8
%ALIGN-3-TRACE:
-Traceback= 418FC0E0 4026B644 40699284 40699A3C 40699368 40E80B84 40E7215C 4068A8AC
```

Conditions: This symptom is observed immediately after an MFR interface is created, after a switchover has occurred, or when a link flaps continuously.

Workaround: There is no workaround.

- CSCeg57219

Symptoms: You cannot ping with packets of certain sizes after an RPR+ switchover or after an interface flap on a multilink interface that has members of non-channelized port adapters when the multilink interface is configured with fragmentation and interleaving.

Conditions: This symptom is observed on a Cisco 7500 series and Cisco 7600 series.

Workaround: There is no workaround.

- CSCeg57482

Symptoms: The SNMP IDBs for the ATM layer that is attached to the main interface are not deregistered when you perform an OIR of a line card. The SNMP IDBs that are attached to the subinterfaces are handled properly.

Conditions: This symptom is observed on a Cisco 12000 series but may also occur on other platforms.

Workaround: There is no workaround.

- CSCeg69793

Symptoms: When an SSO switchover occurs on a customer edge (CE) router, the following error message may be generated for a 4-port OC-3 ATM line card that is processing traffic:

```
%C10K-3-LC_ERR:4oc3atm-1 SAR:delete VC, invalid channel handle
```

Conditions: This symptom is observed on a Cisco 10000 series that functions as a CE router when the 4-port OC-3 ATM line card is configured with more than 500 PVC interfaces and APS is enabled. The symptom occurs rarely and appears to be related to a scaling issue.

Workaround: There is no workaround.

- CSCeh32706

Symptoms: An inter-AS TE LSP fails to send a signal after a router is rebooted as an ASBR.

Conditions: This symptom is observed when there are parallel links between ASBRs with a combination of point-to-point and broadcast interfaces that are configured with the MPLS Traffic Engineering--Inter-AS TE feature and (passive) link flooding.

Workaround: Shut down the broadcast interface between the ASBRs.

- CSCeh35422

Symptoms: A PRP switchover causes “%SYS-2-NOTQ” and “%SYS-2-LINKED” error messages and some tracebacks to be generated on a 1-port channelized OC-12c/STM-4 (DS1/E1) ISE line card, the serial interfaces of the line card flap, and eventually the line card resets.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S or Release 12.0(30)S, that is configured with two PRPs, and that has the redundancy mode set to SSO.

Workaround: There is no workaround.

- CSCeh82547

Symptoms: Tracebacks are generated when a sweep ping is executed on a 24-port channelized E1/T1 line card.

Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.0(30)S or Release 12.0(30)S4.

Workaround: There is no workaround.

- CSCei05246

Symptoms: After an OIR of a PA-MC-E3 port adaptor that is installed in a VIP6-80, the serial interfaces do not transmit. The message “not transmitting” is generated, followed by “output frozen.” After these messages, a Cbus Complex occurs.

Conditions: This symptom is observed on a Cisco 7500 series.

Workaround: There is no workaround.

- CSCei07381

Symptoms: On a 4-port OC-48 POS Engine 4+ line card, a standard or extended access list does not deny IP packets when another link on the same line card is configured for MPLS LDP and when the router is configured for MPLS Explicit Null label support.

Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of Cisco IOS Release 12.0(30)S3 or Release 12.0(31)S.

Workaround: Remove the support for MPLS Explicit Null labels.

- CSCei30764

Symptoms: A PE router that is configured with many (100 or more) Multicast VRFs (mVRFs) may create multiple MDT tunnels for one mVRF.

Conditions: This symptom is observed when you reload a Cisco router that functions as a PE router and that is configured for MVPN.

Workaround: There is no workaround.

- CSCei31560

Symptoms: When a multilink bundle is configured on a 6-port channelized T3 line card, the delay for traffic in the priority queue may be 12 to 14 milliseconds more than what you would expect.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0S when a multilink protocol such as MFR or MLP is configured and when congestion occurs.

Workaround: There is no workaround.

- CSCei39383

Symptoms: Interface configuration parameters are not applied to the running configuration after an RPR+ switchover.

Conditions: This symptom is observed intermittently on a Cisco 12000 series that is configured with a 1-port CHOC-48 ISE line card but may also occur with other line cards.

Workaround: Apply the configuration manually to the affected interface.

- CSCei40506

Symptoms: Performance drops to 90 percent when the “N flag” is set incorrectly for the MDFS process.

Conditions: This symptom is observed on a Cisco 12000 series that is configured for mVPN, that uses an Engine 3 line card for imposition, and that uses an Engine 4+ line card for disposition.

Workaround: Reload the router.

- CSCei41469

Symptoms: The standby PRP crashes when you apply an IPv6 ACL on an interface of an ISE line card.

Conditions: This symptom is observed on a Cisco 12000 series that is configured with redundant PRPs.

Workaround: There is no workaround.

- CSCei48728

Symptoms: New subinterfaces and duplicate IP addresses are unexpectedly created for member interfaces of a port-channel subinterface.

Conditions: This symptom is observed on a Cisco 12000 series that is configured with dual Route Processors that function in RPR mode when a clock and scheduler card (CSC) is shut down before an RPR switchover occurs.

Workaround: There is no workaround.

- CSCei51504

Symptoms: When you run an SNMP get or walk on the ifOperStatus object on a 1-port CHOC-12 OC-3 ISE line card, the status for the STS-1 path interface shows down although the channel is up.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S3.

Workaround: There is no workaround.

- CSCei58551

Symptoms: A 1-port OC-192 Engine 4+ line card (OC192E/POS) or a Modular GbE Engine 4+ line card (EPA-GE/FE-BBRD with EPA-3GE-SX/LH-LC) may crash when an SSO switchover occurs or when the router reloads.

Conditions: This symptom is observed on a Cisco 12000 series that runs a c12kprp-p-mz image of Cisco IOS Release 12.0(31)S and that has two RPs.

Workaround: There is no workaround.

- CSCei62762

Symptoms: Router may generate and/or forward crafted IP packets with the source IP address being the routers tunnel interface for GRE or mGRE tunnels. Incorrect packet decoding may be seen with “debug tunnel.”

Conditions: The router needs to receive a specially crafted GRE packet sent to the tunnel end-point. The outer IP packet must come from the configured tunnel source and be sent to the configured tunnel destination IP address Present Routed bit must be set to 1.

Workaround: Upgrade Cisco IOS to a version containing fixes for: CSCuk27655 or CSCea22552 or CSCei62762.

Further information: On the 6th September 2006, Phenoelit Group posted an advisory:

* Cisco Systems IOS GRE decapsulation fault

Cisco’s statement and further information are available on the Cisco public website at:

<http://www.cisco.com/warp/public/707/cisco-sr-20060906-gre.shtml>

- CSCei69875
Symptoms: Hardware multicast forwarding does not function.
Conditions: This symptom is observed on a Cisco 12000 series after you have reloaded the router.
Workaround: Remove and re-apply hardware multicast forwarding.
- CSCei84343
Symptoms: IP packets that are forwarded from an Engine 6 interface on a Cisco 12000 series to an iBGP route may not reach the destination node.
Conditions: This symptom is observed when the Engine 6 interface forwards these packets as IP packets even though there is a labeled path to the BGP next hop. The output of the **show cef** command shows that the router uses the MPLS labeled path but the Engine 6 hardware is programmed to forward the packets as IP packets instead of MPLS packets. The next router that receives these IP packets may drop them because the next router may be unaware of the iBGP route.
Workaround: There is no workaround.
- CSCei88954
Symptoms: The fourth rule of a standard ACL is ignored.
Conditions: This symptom is observed on a Cisco 10000 series that is configured with a PRE1 and that runs Cisco IOS Release 12.0(24)S or a later release only when a standard ACL is defined with exactly four rules and when this ACL is used for inbound security checking.
Workaround: Define an extra rule that is similar to an earlier rule, perhaps with a different level of masking, to ensure that the ACL has five rules.
- CSCej00097
Symptoms: Interfaces on a Cisco 10000 series 1-port channelized OC-12 line card may take too much time to recover after an PRE switchover has occurred.
Conditions: This symptom is observed when the line card is configured with E1 interfaces that function in SDH mode and is most likely to occur when the line card was previously configured with T1 interfaces that functioned in SONET mode. When a PRE switchover occurs, it may take as long as 60 seconds for all of the interfaces to come back up.
Workaround: There is no workaround.
- CSCej07539
Symptoms: Multicast traffic does not resume fully after you have removed the active PRP from the router.
Conditions: This symptom is observed on a Cisco 12000 series that runs the c12kprp-p-mz image of Cisco IOS Release 12.0(28)S4 and that is configured with redundant PRPs that function in RPR+ mode. The router has two channelized OC-12 line cards that are configured with mVPNs.
Workaround: There is no workaround.
- CSCej09234
Symptoms: The standby RP on a Cisco 12000 series may fail to come up and crash during initialization. The primary RP may generate the following error message:

```
%MBUS-6-DEADSCDY: Standby RP in slot <x> timed out.
```


Conditions: This symptom is observed only when there is a large number of files for the standby RP on the flash disk (for example, when a 1 GB flash disk is about half full) and when the average file size is also large.
Workaround: Delete files on the flash disk.

- CSCej14847

Symptoms: Auto-RP messages from a CE router are lost.

Conditions: This symptom is observed when you enter the **clear ip mroute *** on a connected PE router. The messages do not recover by themselves.

Workaround: To restart Auto-RP messages, enter the **clear ip mds linecard** command.

Alternate Workaround: To restart Auto-RP messages, debug the VRF Auto-RP by entering the **debug ip pim vrf vrf-name auto-rp**.

- CSCej15698

Symptoms: The output of the **show ip mroute vrf vrf-name active** command shows an incorrect entry or rate for decapsulated traffic.

Conditions: This symptom is observed on a Cisco 12000 series that is configured for mVPN.

Workaround: There is no workaround.

- CSCej32588

Symptoms: An interface of an Engine 6 line card is no longer shut down after an RP switchover occurs.

Conditions: This symptom is observed on a Cisco 12000 series when the following events occur:

1. The interface of the Engine 6 line card is configured with the **no shutdown** interface configuration command in the startup configuration.
2. The router is reloaded and you verify that the interface comes up.
3. You enter the **shutdown** interface configuration command on the interface.
4. You enter the **write memory** command.
5. You enter the **redundancy force** command.

After the new RP comes up, the interface appears no longer shut down and the interface comes up again.

Workaround: After you have entered the **shutdown** interface configuration command on the interface followed by the **write memory** command, reload the router.

- CSCej40549

Symptoms: A primary SR-APS physical interface may flap for several minutes in a scaled configuration with 1000 VCs that are configured while the router boots.

Conditions: This symptom is observed on a Cisco 12000 series that runs the c12kprp-p-mz image, that is configured with a 4-port OC-3 ATM ISE line card or 4-port OC-12 ATM ISE line card, and that has SR-APS enabled.

Workaround: There is no workaround.

- CSCej42144

Symptoms: A service policy on an Engine 4 + or Engine 6 line card is incorrectly rejected with the following error message:

```
%E4P and E6 LC requires to configure POLICE and SET %command in every class if either of these two commands %is configured in class-default class
```

This situation occurs when a **set** command is used in all classes.

Conditions: This symptom is observed on a Cisco 12410 that runs Cisco IOS Release 12.0(28)S3, that is configured with dual Performance Route Processors (PRP-1s) that operate in SSO mode, and that has multiple E4+ and/or Engine 6 line cards.

Workaround: There is no workaround.

- CSCej43126

Symptoms: When you reload a 1-port channelized OC-12 ISE line card, all traffic over the line card may be dropped, and an error message and traceback similar to the following may be generated:

```
%IPCGRP-3-SYSCALL: System call for command 14 (slot7/0) : ipc_send_rpc_blocked
timed-out (Cause: timeout) -Traceback= 1F9F20 1FA028 491DC4 49291C 492D08 2E17EC
```

Conditions: This symptom is observed on a Cisco 12000 series that runs an interim release for Cisco IOS Release 12.0(32)S and that functions in a scaled configuration.

Workaround: Reload the router. If this is not an option, there is no workaround.

- CSCej69557

Symptoms: After you reload a PE router that functions in an MVPN topology and that is configured for sparse mode and Auto-RP, the router may not learn the Auto-RP that is advertised by both a local and remote CE router, preventing traffic from resuming to flow.

Conditions: This symptom is observed on a Cisco 12000 series that runs an interim release for Cisco IOS Release 12.0(32)S and that functions as a PE router. The symptom may also occur in other releases of Release 12.0S.

Workaround: Enter the **clear ip mds line** command.

- CSCej82265

Symptoms: An MPLS TDP peer is down.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S3 and that has the **mpls ldp protocol tdp** command configured on the interface on which TDP peering cannot be established. The peer router has the **mpls ldp protocol both** command configured.

Workaround: Enter the **mpls ldp protocol tdp** command on the peer router. Note that this workaround may not be plausible for routers that run a legacy Cisco IOS software that only supports TDP.

- CSCej86175

Symptoms: In a multicast VPN (MPVN) environment, when a Stateful Switchover (SSO) occurs on a PE router, the multicast traffic in the MVRF does not recover because the neighboring PE router fails to re-establish its PIM neighbor relationship. Note that the symptom does not occur for unicast traffic.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S2 or an interim release for Release 12.0(32)S and that functions as a PE router (PE1) in the following topology:

```
multicast origination --> PE2 --> PE1 --> CE1 --> multicast termination
```

When an SSO occurs on PE1, PE2 does not re-establish its PIM neighbor relationship with PE1 in the MVRF. PE1 and PE2 are global PIM neighbors.

Workaround: Reload PE1.

Further Problem Description: When the symptom occurs, PE1 still shows PE2 as its PIM neighbor in the MVRF. Clearing the multicast route in the MVRF does not help to resolve this issue.

- CSCek05730

Symptoms: A Cisco 7200 series that runs Cisco IOS Release 12.0(31)S1 may crash unexpectedly because of a bus error and/or display some spurious memory accesses.

Conditions: This symptom is observed when an interface that is configured for some form of fancy queueing (that is, anything besides FIFO queueing) actively forwards traffic.

Workaround: Disable fancy queueing on the Ethernet interface.

- CSCek08638

Symptoms: Data traffic that is received by a provider edge (PE) router on an Ethernet port may not be forwarded over an L2TPv3 tunnel.

Conditions: This symptom is observed on a Cisco 12000 series when the line card that faces the customer edge (CE) router is one of the following line cards:

- 8-port Fast Ethernet, 100BASE-FX line card (8FE-FX-SC-B)
- 8-port Fast Ethernet, 100BASE-TX line card (8FE-TX-RJ45-B)
- 1-port Gigabit Ethernet line card (GE-GBIC-SC-B)

Workaround: There is no workaround.

- CSCek24821

Symptoms: The memory of a SIP-400 depletes entirely, and the following error message is generated:

```
EE48-3-ALPHA_MCAST: Can't assign new hw_mdb - (S,G)=(<IP>), mi=431, side=TX
```

Conditions: This symptom is observed on a Cisco 12000 series that functions as a PE router when the following conditions are present:

- The router receives traffic with invalid sources, that is the traffic is sent from sources that are not in the global routing table, causing RPF to fail.
- (S,G) information is still created for the invalid sources, and when the (S,G) information times out, the memory of the SIP-400 is not released.
- Regular traffic comes from a valid source and is directed to the same group address.
- The non-RPF source has a hash collision with the valid traffic stream.

Workaround: There is no workaround.

- CSCek25127

Symptoms: There is no IPv4 BGP MPLS functionality between BGP peers.

Conditions: This symptom is observed on a Cisco 12000 series that is connected to a BGP peer over a link bundle interface.

Workaround: There is no workaround.

- CSCek27756

Symptoms: All interfaces of a 24-port channelized E1/T1 line card flap.

Conditions: This symptom is observed on a Cisco 10000 series when extensive channel reprovisioning is configured on the line card.

Workaround: Perform a microcode reload for the line card and then reset the line card.

- CSCek28323

Symptoms: An interface of an Engine 3 ingress line card that functions in feature mode may become stuck, and all traffic may be dropped.

Conditions: This symptom is observed on a Cisco 12000 series that is configured with an Engine 3 ingress line card that has the **hw-module slot slot-number np mode feature** command enabled and that is configured with an egress line card that has a link bundle interface.

Workaround: Disable the **hw-module slot *slot-number* np mode feature** command on the Engine 3 ingress line card.

- CSCin91381

Symptoms: A VIP that has a dMLFR configuration may crash when you enter the **microcode reload** global configuration command.

Conditions: This symptom is observed on a Cisco 7500 series when traffic flows through the VIP.

Workaround: There is no workaround.

- CSCin95125

Symptoms: dCEF switching does not function when Frame Relay over L2TPv3 is configured on a 2-port OC-3 POS port adapter (PA-POS-2OC3) that is installed in a VIP 6-80.

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(30)S3 when an interface of the PA-POS-2OC3 faces the core of the network. When traffic from the core leaves the PA-POS-2OC3 to a CE router, dCEF switching functions fine. However, when traffic from the CE router leaves the PA-POS-2OC3 to the core, dCEF switching does not function and the VIP 6-80 punts the traffic to the RSP.

Workaround: There is no workaround.

- CSCin96583

Symptoms: After an OIR of a VIP on a Cisco 7500 series, MLP traffic causes a very heavy CPU load on the RP, in turn causing failures in the IPC configuration and memory allocation (malloc) failures.

Conditions: This symptom is observed on a Cisco 7500 series that is configured with a large number of distributed MLP bundles.

Workaround: There is no workaround.

- CSCin96692

Symptoms: On a Cisco 7500 series that is configured for dMLP, the txacc values of member interfaces may be wrongly credited to other member interfaces, causing RSP-3-RESTART messages, and finally causing traffic to stop.

Conditions: This symptom is observed when the member links flap continuously for some time while traffic is being processed.

Workaround: There is no workaround.

- CSCsa75484

Symptoms: After an SSO has occurred, all packets are received but not forwarded to the PXF engine, preventing pings from going through.

Conditions: This symptom is observed on a Cisco 10000 series that is configured with a 1-port Gigabit Ethernet half-height line card.

Workaround: There is no workaround.

- CSCsa91478

Symptoms: A Cisco 12000 series that is configured for L2TPV3 may continuously log the following CM_ERROR message, causing the syslog server to be flooded:

```
%SW_MGR-3-CM_ERROR: Connection Manager Error - unprovision segment failed
%SW_MGR-3-CM_ERROR: Connection Manager Error - unprovision segment failed
```

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(30)S1 when a Multilink Frame Relay (MFR) interface is shut down in the configuration of the **connect** command, causing proper provisioning to fail, unprovisioning to occur, and the error message to be generated.

Possible Workaround: Enter the **no shutdown** interface configuration command on the MFR interface.

- CSCsb11124

The Cisco IOS Stack Group Bidding Protocol (SGBP) feature in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable denial of service condition. Devices that do not support or have not enabled the SGBP protocol are not affected by this vulnerability.

Cisco has made free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability.

Cisco has published a Security Advisory on this issue; it is available at <http://www.cisco.com/warp/public/707/cisco-sa-20060118-sgbp.shtml>

- CSCsb12969

Symptoms: All VIPs or FlexWAN modules reload unexpectedly on a platform that is configured for Modular QoS CLI (MQC).

Conditions: This symptom is observed on a Cisco 7500 series (with VIPs) and a Cisco 7600 series and Cisco Catalyst 6500 series (both with FlexWANs) when the following steps occur while the physical interface is in the UP state:

1. An input policy and output policy map are already attached to an ATM or Frame Relay PVC. When you attach the same policy map to the main interface, an error message is generated and the configuration is rejected.
2. You remove the policy map from the PVC and attach the same policy map to the main interface.
3. You remove the policy map from the main interface.

At this point, all VIPS or FlexWAN modules reload, even though no traffic is being processed during the above-mentioned steps.

Workaround: There is no workaround.

- CSCsb28139

Symptoms: An LDP/BGP adjacency is not formed, and a ping does not go through.

Conditions: This symptom is observed on a Cisco 12000 series that functions in a scaled VPN environment when an Engine 6 line card faces the core of the MPLS network.

Workaround: Enter the **clear ip route *** command.

- CSCsb39165

Symptoms: A Cisco router may report high CPU usage and memory depletion under a specific MPLS VPN configuration with static routes.

Conditions: This symptom is observed when equal cost static routes to a subnet point to a next hop address and there is a summary route that covers one of the next hops pointing to Null0.

If the directly connected route to the next hop is terminated because the interface goes down, the original route recurses to Null0 while the route recursing through the interface that is still up remains in the routing table. The end result is that the route now points to both Null0 and to a valid interface that is up, causing an MPLS recursion problem that results in high CPU usage and memory depletion.

The following is an example configuration:

```
ip route a.a.a.a b.b.b.b y.y.y.y
ip route a.a.a.a b.b.b.b z.z.z.z
ip route y.y.y.y mask Null0
```

If the directly connected route y.y.y.y is removed the a/b subnet recurses through the y.y.y.y/mask route to Null0.

Workaround: Use routes that point to both a next hop and an egress interface, as in the following example:

```
ip route a.a.a.a b.b.b.b interfaceY y.y.y.y
ip route a.a.a.a b.b.b.b interfaceZ z.z.z.z
```

- CSCsb44645

Symptoms: A nested policy map may not function as expected.

Conditions: The symptom is observed when an action is removed from a class map that has multiple actions in the last level of a nested policy map.

Workaround: First detach the policy from the interface, remove the action, and then re-attach the policy to the interface.

- CSCsb46607

Symptoms: A standby route processor (RP) may crash in the “CEF LC IPC Background” process.

Conditions: This symptom is observed on a Cisco platform when an SSO switchover occurs.

Workaround: There is no workaround.

- CSCsb59555

Symptoms: An Engine 3 or Engine 4+ line card may be stuck in the “request reload” state and CEF may be disabled on the line card, although the CEF table is up, as is shown in the output of the **show cef linecard** command:

Slot	MsgSent	XDRSent	Window	LowQ	MedQ	HighQ	Flags
1	8558	719895	4966	0	0	0	up
2	8560	718293	4966	0	0	0	up
3	8609	722867	4965	0	0	0	up
4	8584	721311	4965	0	0	0	up
5	8597	724307	4965	0	0	0	up
9	8586	722060	4966	0	0	0	up
10	8579	720566	4966	0	0	0	up
11	8566	719086	4966	0	0	0	up
12	8606	725072	4966	0	0	0	up
13	8597	723572	4966	0	0	0	up
*7	1	3	24	0	0	0	disabled, rrp hold
0	4058	359354	4966	0	0	0	up

VRF Default, version 5032, 5024 routes

Slot	Version	CEF-XDR	I/Fs	State	Flags
1	5032	5016	67	Active	sync, table-up
2	5032	5016	5	Active	sync, table-up
3	5032	5016	20	Active	sync, table-up
4	5032	5016	5	Active	sync, table-up
5	5032	5016	5	Active	sync, table-up
9	5032	5016	4	Active	sync, table-up
10	5032	5016	4	Active	sync, table-up

11	5032	5016	20 Active	sync, table-up
12	5032	5016	4 Active	sync, table-up
13	5032	5016	8 Active	sync, table-up
*7	0	0	4 Active	table-disabled
0	0	0	5 Active	request reload, table-up

Conditions: This symptom is observed on a Cisco 12000 series after an RPR+ switchover has occurred. However, the symptom is platform-independent and may also occur on another platform that is configured for CEF when an RPR+ switchover has occurred.

Workaround: Enter the **clear cef linecard** command for the affected line card.

- CSCsb83876

Symptoms: The counters on a PA-MC-E3 port adapter may provide incorrect information. For some interfaces of the port adapter, the counters are always zero, and for others interfaces, the counters do increase but very slowly.

Conditions: This symptom is observed when you enter the **show interfaces type slot** command for a PA-MC-E3 port adapter.

Note that the symptom does not occur when you enter the **show interface type number stats** command or the **show interfaces type slot accounting** command. Also, when you enter the **show interfaces type slot** command for the VIP in which the PA-MC-E3 port adapter is installed, the counters provide correct information.

Workaround: Enter the **show interface type number stats** command to retrieve the correct information.

- CSCsb88907

Symptoms: A Cisco 12000 series RP crashes when you enter the **clear l2tun all** command.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(30)S3 when the **debug vpdn l2x-packets** command is enabled on the router.

Workaround: Do not enter the **clear l2tun all** command when the **debug vpdn l2x-packets** command is enabled on the router.

- CSCsb98254

Symptoms: A router may fail when you reload a Gigabit Ethernet (GE) line card or port adapter that has link-bundling enabled.

Conditions: This symptom is observed on a Cisco router when dot1q is configured on a GE interface of the line card or port adapter and when MPLS is enabled on an uplink.

Workaround: There is no workaround.

- CSCsc08181

Symptoms: The PXF engine reloads when you enter the **service-policy output** command.

Conditions: This symptom is observed on a Cisco 10000 series router when the following conditions are present:

- The **frame-relay fragment** command is configured on a Frame Relay interface.
- An output service policy that has the **bandwidth**, **priority**, or **shape** command enabled is applied to a Frame Relay permanent virtual circuit (PVC).

Workaround: Do not combine interface-based Frame Relay fragmentation with a PVC-based service policy. Rather, either apply both Frame Relay fragmentation and a service policy to the physical interface or apply both Frame Relay fragmentation and a service policy to the Frame Relay PVC.

- CSCsc18258

Symptoms: When you attempt to attach a child service policy to a parent shaper on a 4-port GE ISE line card, the configuration is rejected with the following error message:

```
% Not enough bandwidth resources on interface GigabitEthernet3/0.275 to satisfy request.
```

In this context, the error message is supposed to mean that the guaranteed bandwidth of the child policy exceeds the rate of the parent shaper. However, when the symptom occurs, the configuration is rejected even when the child bandwidth is less than the parent shaper rate.

Conditions: This symptom is observed on a Cisco 12000 series after the child policy is added and removed a number of times and occurs because of leaking bandwidth in the bandwidth management.

Workaround: There is no workaround. To clear the symptom, reload the affected line card.

- CSCsc30289

Symptoms: When the router at the opposite site is reloaded, a Dynamic Packet Transport (DPT) line card crashes because of a “Bus Error exception.”

Conditions: This symptom is observed on a Cisco 12000 series when the router at the opposite site is also configured with a DPT line card.

Workaround: There is no workaround.

- CSCsc30648

Symptoms: A POS line card that is configured with third-party vendor Small Form-Factor Pluggable Interface Converters (SFPs) and that is installed in a Cisco 12000 series fails the security check.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(30)S3 or Release 12.0(31) during the initial boot process.

Note that when the router runs Release 12.0(28)S3 and you boot the router with the SFPs already installed, the symptom does not occur. However, when you reload the router and then remove and reinsert the SFPs, they do not pass the security check either.

Workaround: There is no workaround.

- CSCsc37404

Symptoms: An Engine 6 line card may reset with the following error messages:

```
%IPC-5-INVALID: NACK Source Port=0x403F0000
%MCC192-3-CPU_PIF: Error=0x4 %MCC192-3-CPUIF_ERR: Packet Exceeds Programmed Length.
%GSR-3-INTPROC: Process Traceback= 40D32E5C 406D8CE0 ...
```

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S2.

Workaround: There is no workaround.

- CSCsc37572

Symptoms: When you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on MFR interfaces that are configured on a 1-port channelized OC-12/STM-4 (DS1/E1) ISE line card, traffic may not longer be forwarded.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(30)S4.

Workaround: Reload the 1-port channelized OC-12/STM-4 (DS1/E1) ISE line card.

- CSCsc44237

This caveat consists of two symptoms, two conditions, and two workarounds:

1. Symptom 1: A switch or router that is configured with a PA-A3 ATM port adapter may eventually run out of memory. The leak occurs when the FlexWAN or VIP that contains the PA-A3 port adapter is removed from the switch or router and not re-inserted.

The output of the **show processes memory** command shows that the “ATM PA Helper” process does not have sufficient memory. The output of the **show memory allocating-process totals** command shows that the “Iterator” process holds the memory.

Condition 1: This symptom is observed on a Cisco switch or router that runs a Cisco IOS software image that contains the fixes for caveats CSCeh04646 and CSCeb30831. A list of the affected releases can be found at

<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeh04646> and

<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeb30831>.

Cisco IOS software releases that are not listed in the “First Fixed-in Version” fields at these locations are not affected.

Workaround 1: Either do not remove the PA-A3 ATM port adapter from the FlexWAN or VIP or re-insert the PA-A3 ATM port adapter promptly. The memory leak stops immediately when you re-insert the PA-A3 ATM port adapter.

2. Symptom 2: A switch or router that has certain PIM configurations may eventually run out of memory.

The output of the **show processes memory** command shows that the “PIM process” does not have sufficient memory. The output of the **show memory allocating-process totals** command shows that the “Iterator” process holds the memory.

Condition 2: This symptom observed on a Cisco router that runs a Cisco IOS software image that contains the fix for caveat CSCef50104.

A list of the affected releases can be found at

<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCef50104>. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

Workaround 2: When the **ip multicast-routing** command is configured, enable at least one interface for PIM. When the **ip multicast-routing vrf vrf-name** command is configured, enter the **ip vrf forwarding vrf-name** command on at least one interface that has PIM enabled.

- CSCsc46474

Symptoms: When you create a VRF, a router generates the following error message for a link bundle that does support MPLS VPN and that is configured on a 3-port Gigabit Ethernet (GE) Engine 2 line card:

```
%LC-6-PSA_UCODE_NO_SUPPORT: Current bundle does NOT support (MPLS VPN)
```

When you apply the VRF to an interface of the 3-port GE Engine 2 line card by entering the **ip vrf forwarding** command, the 3-port GE Engine 2 line card crashes.

Conditions: These symptoms are observed on a Cisco 12000 series that is configured with a port channel for link bundling.

Workaround: There is no workaround.

- CSCsc58973

Symptoms: When the **mpls ping** and **traceroute** commands are configured, the specified destination address does not take effect, nor is the 127.0.0.1 default address used when the destination address is not specified. Instead, the target FEC is used as the destination IP address in IP header of the outgoing packet.

When you specify a range of destinations for troubleshooting, the target IP address is always used. This situation prevents you from using the **mpls ping** and **traceroute** commands to troubleshoot an equal-cost multipath (ECMP) configuration.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0S.

Workaround: There is no workaround.

- CSCsc63558

Symptoms: A 2-port OC-192 POS Engine 6 line card (the 2OC192/POS-SR-SC and the 2OC192/POS-IR-SC) may stop forwarding traffic after running properly for a while. When this situation occurs, the POS interface is in the UP/UP state, but a ping to the directly connected POS interfaces fails. No error messages are generated for the affected line card.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S2 or Release 12.0(28)S5, irrespective of whether or not an ACL is configured on the line card.

Workaround: There is no workaround. You must reset the line card to recover from the symptoms.

- CSCsc64723

Symptoms: After an SSO switchover, traffic does not fully recover on a 3-port GE Engine 2 line card that is configured for EoMPLS.

Conditions: This symptom is observed on a Cisco 12000 series that runs the c12kprp-p-mz image of Cisco IOS Release 12.0(28)S5.

Workaround: Enter the **clear cef linecard slot-number** command to recover from the symptom and enable traffic to pass properly.

- CSCsc65300

Symptoms: The line protocol flaps on the E1 interfaces of a 24-port channelized E1/T1 line card.

Conditions: This symptom is observed on a Cisco 10000 series.

Workaround: Initiate a PRE switchover to restore the stability of the router.

- CSCsc73112

Symptoms: On a Cisco 10000 series 4-port OC-3 ATM line card, a flowbit offset mismatch may occur on certain PVCs when you enter the **shutdown** interface configuration command on an ATM subinterface before you remove a service policy from the ATM subinterface.

Conditions: The symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.0(30)S4 and that is configured with a PRE1 when about 400 PVCs are activated on the line card.

Workaround: Do not enter the **shutdown** interface configuration command on the ATM subinterface before you remove the service policy.

- CSCsc88940

Symptoms: After an RPF interface change occurs, the RPF check passes always on port 0 of an Engine 2 line card. This situation causes non-RPF traffic to be forwarded via the RPF interface and causes multicast traffic with a valid RPF (S,G) to be duplicated.

Conditions: This symptom is observed on a Cisco 12000 series and occurs because of an error during the calculation of the RPF interface.

Workaround: Do not use port 0 of an Engine 2 line card for multicast traffic in a configuration in which RPF interface changes may occur in such a way that port 0 receives non-RPF traffic.

- CSCsc89167

Symptoms: An inconsistency may occur in how CEF treats a recursive route on the PXF engine.

Conditions: This symptom is observed on a Cisco 10000 series.

Workaround: Configure a static ARP entry for the next hop.

First Alternate Workaround: Increase the timeout for the next hop,

Second Alternate Workaround: Ping from the RP of the Cisco 10000 series to the next hop to resolve the adjacency.

- CSCsc99111

Symptoms: The following QoS configuration commands fail to complete, causing the platforms that they are running on to hang:

- the **policy-map** command, including any commands in submodes under the **policy-map** command.
- the **class-map** command, including any commands in submodes under the **class-map** command.
- the **service-policy** command.

Conditions: This symptom is observed when the **show policy-map interface** command is run before the QoS configuration command is entered and when either one of the following conditions is present:

- The **show policy-map interface** command includes the *input* argument and only an output service policy is present on the interface.
- The **show policy-map interface** command includes the *output* argument and only an input service policy is present on the interface.

Workaround: There is no workaround. To prevent the symptom from occurring, enter the **show policy-map interface** command without the *input* or *output* argument. Doing so displays all service policies that are attached to the interface. Input and output policies are labeled as such in the command output.

Further Problem Description: Locks are used to control access to the QoS configuration database. This ensures that QoS **show** and configuration commands function against consistent views of the configuration data.

In the case of the **show policy-map interface** command, it is possible for the lock to be acquired but not released under the special case that is described in the Conditions section above. This situation occurs because of omissions in two error handling code paths that are triggered when a service policy is present only in the opposite direction from the direction that the **show policy-map interface** command requests.

Once the lock has been “orphaned” in this fashion, subsequent QoS configurations wait indefinitely for the lock to be released.

Other QoS **show** commands are not affected and continue to run normally.

- CSCsd11701

Symptoms: When multicast hardware acceleration is enabled, a wrong label stack may be imposed on packets that have an IP destination address below 16.x.x.x. This situation occurs, for example, when the IP destination address is 10.1.1.1 and when the ingress interface is an MPLS VPN VRF subinterface that is configured for 802.1q. Note that in this situation, the CEF forwarding information is correct, that is, it has the correct label stack.

Conditions: This symptom is observed on a Cisco 12000 series that is configured with a 3-port GRE Engine 2 line card but may occur on any Engine 2 line card that has VRF interfaces. The symptom occurs only when multicast hardware acceleration is enabled.

A list of the affected releases can be found at

<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCEi01644>. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

Workaround: There is no workaround.

- CSCsd14677

Symptoms: Link under-utilization may occur on an ATM PVC, and packet drops may occur when traffic is processed at a lower value than the Peak Cell Rate (PCR).

Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.0(30)S and that is configured with a PRE1 and a 4-port OC3 ATM line card. The line card is configured for oversubscription factor 50.

Workaround: There is no workaround.

- CSCsd23362

Symptoms: When MLP interfaces on a 1-port channelized OC-12/STM-4 (DS1/E1) ISE line card are configured for MVPN and you reload the router, the PIM VRF neighbor may not be established via a tunnel for some MLP interfaces.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(30)S4.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected MLP interfaces.

- CSCsd24601

Symptoms: The FIB becomes disabled when you bring down a member link of an MLP or MFR bundle.

Conditions: This symptom is observed on a Cisco 7500 series that is configured with an MLP or MFR bundle and that runs Cisco IOS Release 12.0(30)S, Release 12.0(31)S, or Release 12.0(32)S, all of which integrate the fix for caveat CSCeg57219. Other Cisco IOS software releases that integrate the fix for caveat CSCeg57219 are not affected.

Workaround: There is no workaround.

- CSCuk45823

Symptoms: A router may reload when a high load of IP version 6 (IPv6) multicast traffic is being forwarded. The symptom occurs because of a corrupted redzone in the packet memory.

Conditions: This symptom is observed only on the i82543-based Ethernet family of controllers.

Workaround: Disable IPv6 multicast.

Wide-Area Networking

- CSCsb61367

Symptoms: When you enter the **redundancy force-switchover** command on a router that is configured for PPP encapsulation, the IS-IS neighbor comes up in the INIT state.

Conditions: This symptom is observed on a Cisco router that is configured with two RPs that run in SSO redundancy mode.

Workaround: To bring up the IS-IS state in the IS-IS neighbor, enter the **isis protocol shutdown** interface configuration command followed by the **no isis protocol shutdown** interface configuration command on interface that provides the connection to the IS-IS neighbor.

Alternate Workaround: Configure HDLC encapsulation on the router.

Resolved Caveats—Cisco IOS Release 12.0(30)S4

Cisco IOS Release 12.0(30)S4 is a rebuild of Cisco IOS Release 12.0(30)S. The caveats listed in this section are resolved in Cisco IOS Release 12.0(30)S4 but may be open in previous Cisco IOS releases. This section describes only severity 1, severity 2, and select severity 3 caveats.

Basic System Services

- CSCsb08386

Symptoms: A router crashes when you enter the **show ip bgp regexp** command.

Conditions: This symptom is observed on a Cisco router when BGP is being updated.

Workaround: Enable the new deterministic regular expression engine by entering the **bgp regexp deterministic** command and then enter the **show ip regexp** command. Note that enabling the new deterministic regular expression engine may impact the performance speed of the router.

- CSCsb14371

Symptoms: A Cisco 7500 series may log the following error message even if no VIP is installed in slot 0:

```
%IPC_RSP_CBUS-3-NOHWQ: Hardware queue for card at slot 0 not found
```

Conditions: This symptom is observed after a crash of another VIP has occurred. Sometimes the symptom occurs when a VIP is installed in slot 0 but most of the time there is no VIP in slot 0 when the symptom occurs.

Workaround: There is no workaround.

Interfaces and Bridging

- CSCeg17576

Symptoms: Traffic loss may occur when you enter the **ip multicast-routing** and **ip pim** commands on an Ethernet interface that is already configured for Xconnect.

Conditions: This symptom is observed only on a Cisco 7200 series and Cisco 7500 series.

Workaround: To enable Xconnect traffic to resume, unconfigure and reconfigure the Xconnect statement on the Ethernet interface.

- CSCin75573

Symptoms: When you perform an OIR of a PA-MC-8TE1+ or PA-MC-8E1 port adapter, the following error message and traceback may be generated:

```
%ALIGN-3-SPURIOUS: Spurious memory access made at 0x60379D34 reading 0xD8 %  
ALIGN-3-TRACE:  
-Traceback= 60379D34 604F1CFC 60BD0664 6032B93C 6039A0CC 6010A908 6032AA7C 6032EBAC
```

Conditions: This symptom is observed on a Cisco router when the port adapter is configured for QOS on an egress serial interface and traffic is flowing through this interface.

Workaround: There is no workaround.

- CSCin86455

Symptoms: Auto-provisioning may be disabled on a Cisco router that is configured with a PA-A3 port adapter.

Conditions: This symptom is observed when a VC class that is configured for create on-demand is attached to the main ATM interface and then the create on-demand configuration is removed and re-applied to the VC class.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the ATM interface of the PA-A3 port adapter.

- CSCsb04481

Symptoms: CEF may fail and the following error message is generated:

```
Interface Serial0/0:63 changed state to down  
%CT3-3-LOVEFAIL: CT3-SW-PA-0/0: failed to send T3 line state change love letter  
%AMD2_FE-5-LATECOLL: Ethernet0/0 transmit error
```

Conditions: This symptom is observed on a Cisco 7500 series that is configured with a channelized T3 port adapter.

Workaround: There is no workaround.

IP Routing Protocols

- CSCdz42920

Symptoms: A router may crash because of a bus error when you configure IP accounting.

Conditions: This symptom is observed when you enter the **clear ip accounting** EXEC command.

Workaround: Do not enter the **clear ip accounting** or **show ip accounting** EXEC command.

- CSCea31201

Symptoms: A Cisco router may reload unexpectedly because of a bus error.

Conditions: This symptom is observed on a Cisco router that has the **ip accounting** interface configuration command enabled.

Workaround: There is no workaround. The problem is rare and typically not reproducible.

- CSCeg52659

Symptoms: A Cisco 7200 series may not withdraw a BGP route from an iBGP peer.

Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.3(3) when the **clear ip bgp neighbor-address soft out** command is entered for one of the members of the peer group of which the Cisco 7200 series is a member and when some changes to the outbound policy are made to the same member of the peer group. This situation causes some prefixes to remain stuck in the other members of the peer group. The symptom may also occur in other releases.

The symptom is a very old behavior of the BGP peer group functionality: when one member of a peer group is cleared via either a hard reset or a soft reset and a policy change causes some of the prefixes to be withdrawn, inconsistencies may occur in the routes on the other members of the peer group.

Workaround: For peer groups and neighbors that are members of a peer group, do not enter the BGP neighbor-specific **clear ip bgp neighbor-address soft out** command or the **clear ip bgp neighbor-address** command. Rather, enter the peer group-specific **clear ip bgp peer-group-name soft out** command or the **clear ip bgp peer-group-name** command.

- CSCeh07809

Symptoms: When BGP nexthop information for a prefix changes because of topology changes, BGP properly updates its path information and IP routing table entry but CEF may not update the corresponding CEF entry, causing a stale entry. This inconsistency between BGP and CEF may cause a connectivity problem.

Conditions: This symptom is observed when the nexthop information changes to an existing prefix entry in the BGP routing table. Typically, this occurs when the interface through which the prefix is learned goes down.

Workaround: Flush out the stale CEF entry by entering the **clear ip bgp** command or withdraw and readvertise the prefix by the source router, which enables the affected router to refresh the CEF entry.

- CSCeh35659

Symptoms: When the **ip bgp fast-external-fallover permit** interface configuration command is enabled on the main interface of a 4-port Gigabit Ethernet ISE line card and on a subinterface of a connected BGP neighbor, and when you enter the **shutdown** interface configuration command on the main interface, the BGP session that is established on the subinterface remains up for about 150 to 180 seconds before the BGP hold timer causes the session to go down.

Conditions: This symptom is observed on a Cisco 12000 series in a per-interface fast external fallover configuration on a 4-port Gigabit Ethernet ISE line card. However, the symptom may also occur on other platforms that function in a BGP configuration.

Workaround: There is no workaround. Note that the **ip bgp fast-external-fallover permit** command is currently not supported on subinterfaces.

- CSCeh53906

Symptoms: A stale non-bestpath multipath remains in the RIB after the path information changes, and BGP does not consider the stale path part of the multipath.

Conditions: This symptom is observed on a Cisco router that has the **soft-reconfiguration inbound** command enabled and occurs only when the BGP Multipath Loadsharing feature is enabled for three or more paths, that is, the *number-of-paths* argument of the **maximum-paths number-of-paths** command has a value of three or more.

Workaround: Disable the **soft-reconfiguration inbound** command for the neighbor sessions for which the BGP Multipath Loadsharing feature is enabled or reduce the maximum number of paths for the BGP Multipath Loadsharing feature to two.

- CSCei06089

Symptoms: Conditional advertisement of the default route via a route map does not work when you enter the **neighbor default-originate** command.

Conditions: This symptom is observed on a Cisco router that is configured for BGP.

Workaround: Disable the route map entirely. If this is not an option, there is no workaround.

- CSCei25454

Symptoms: Connectivity loss may occur for MVPNs.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(30)S or a later release when the MVPNs function in a mixed network that has both VPNv4 RD2 prefixes for MDT updates and IPv4 MDT subaddress family identifier (SAFI) prefixes.

Workaround: There is no workaround.

- CSCei26899

Symptoms: When you reset a BGP peer, some prefixes are missing.

Conditions: This symptom is observed on a Cisco MGX8850 RPM-XF that runs Cisco IOS Release 12.3(11)T. However, the symptom is platform-independent and may also occur in other releases.

Workaround: There is no workaround.

- CSCsa98059

Symptoms: Suboptimal routing occurs in an OSPF configuration or a routing loop occurs between two border routers that redistribute BGP into OSPF.

Conditions: These symptoms are observed when at least two border routers are connected via eBGP to another autonomous system, receive the same prefix over these connections, and redistribute the prefix into OSPF. Under certain conditions, for example when the eBGP session from the preferred BGP exit point to the eBGP peer flaps, the second router in the local autonomous system becomes the preferred path and redistributes the eBGP route into OSPF. When the eBGP session with the first router comes back up, the LSA should be flushed but this does not occur. This situation may create routing problems on other OSPF routers or, when BGP has a higher administrative distance than OSPF, routing loops between both border routers.

Workaround: There is no workaround.

- CSCsb54823

Symptoms: One router (R2) may begin sending updates to another router (R1) before R2 has received the BGP prefix list from R1.

R1 does apply its inbound BGP prefix list so routes are denied if they need to be. However, R2 sends routes to R1 which are denied by R1.

Conditions: This symptom is observed when both routers have negotiated a BGP outbound route filter (ORF) and when R1 sends its BGP prefix list to R2.

Workaround: There is no workaround.

ISO CLNS

- CSCei58655

Symptoms: A route that fails remains in the routing table with its old metric, preventing an alternate route from being used and causing a routing loop.

Conditions: This symptom is observed in a network that is configured for IS-IS and iSPF when the IP routes that are advertised in an LSP (irrespective of whether or not the LSP is fragmented) do not age-out during a rerouting failure.

Workaround: Remove iSPF from the IS-IS process by entering the **router isis** command followed by the **no ispf** command.

Miscellaneous

- CSCdr54486

Symptoms: Traffic is dropped for up to 15 seconds while a recursive prefix is being resolved.

Conditions: This symptom is observed when a new recursive prefix is learned by CEF and when a less-specific prefix already exists. Traffic that would have been forwarded using the less-specific prefix is dropped for up to 15 seconds while the new recursive prefix is being resolved.

Workaround: There is no workaround.

- CSCdz83100

Symptoms: High CPU use may occur at the interrupt level on an ingress port adapter or line card that is configured for hardware multicast when there is a high multicast traffic rate.

Conditions: This symptom is observed when policy-based routing (PBR) matches the multicast traffic and when a switchover to another interface occurs.

Workaround: Change the deny statement in the PBR configuration so traffic for multicast destination addresses is denied earlier.

Alternate Workaround: For a short while, remove the PBR configuration from the ingress interface to enable multicast traffic hardware forwarding to be established.

Further Problem Description: PBR should not influence multicast traffic and it does not when traffic is switched in the hardware. When a switchover to a new interface occurs, multicast packets are initially forwarded in the software until hardware forwarding can take over. PBR interferes with the initial software-switched packets and prevents hardware entries from being created.

- CSCee93598

Symptoms: An LSP ping reports that an LSP is fine although the LSP is unable to carry MPLS payloads such as VPN traffic.

Conditions: This symptom is observed on a Cisco router when MPLS echo request packets are forwarded from untagged interfaces that are directly connected to the destination of the LSP ping and when the IP time-to-live (TTL) value for the MPLS echo request packets is set to 1.

Workaround: There is no workaround.

- CSCeg12134

Symptoms: When you send multicast traffic over an IPSec tunnel, a memory leak may occur on a router.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3T when both IP CEF and hardware encryption are configured. The symptom may also occur in other releases.

Workaround: Switch to software encryption for a while and then switch back to hardware encryption.

Alternate Workaround: Disable IP CEF.

- CSCeg24422

Symptoms: Packet drops occur in the ingress direction on a dMLP or dMLFR link with traffic at 95-percent of the line rate and when the number of packets with a small size is high.

Conditions: This symptom is observed on a Cisco 7500 series that functions as a provider edge (PE) router, that is configured for L2TPv3 L3VPN, and that has dMLP or dMLFR links to a customer edge (CE) router.

Workaround: There is no workaround.

- CSCeg26528

Symptoms: The performance of a router may be severely degraded (at approximately 90 percent of the line rate) when large packets are processed, when the MLP bundle link flaps, and when the router does not recover the MLP sequence numbers of the packets.

Conditions: This symptom is observed on a Cisco 7500 series and Cisco 7600 series that are configured for dMLP only when large packets are processed.

Workaround: There is no workaround.

- CSCeg40957

Symptoms: A router that is equipped with a PA-A3-OC3 ATM port adapter may generate alignment errors.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(25)S1 and that is configured for Xconnect. The symptom may also occur in other releases.

Workaround: There is no workaround.

- CSCeg82322

Symptoms: Platform independent multicast protocol software running in a line card will exit without logging any errors when detecting an illegal value for an input “hardware” interface if_index or an input “software” interface if_number.

A line card may crash or experience other errors whose cause will be difficult to identify.

Conditions: These symptoms only occur when a preceding error has occurred during route processor assignment of interface indices. These errors are frequently accompanied by error messages.

Workaround: Utilize RP error messages if available to diagnose the cause of the problem.

- CSCeh04295

Symptoms: When ATM packets are sent over an 8-port OC-3 ATM Engine 2 line card, the packets are punted to the CPU of the line card, causing traffic drops.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S and that is configured for ATOM when an 8-port OC-3 ATM Engine 2 line card is the disposition card.

Workaround: There is no workaround.

- CSCeh13340

Symptoms: On a Cisco XR 12000 series hardware-based forwarding line card, the receive counters in the output of the **show mpls l2transport vc** command do not work in any images for ATOM.

Conditions: This symptom is observed on all hardware-based engine line cards on a Cisco XR 12000 series that is configured for ATOM and Sampled NetFlow on the core-facing line cards.

Workaround: There is no workaround.

- CSCeh27783

Symptoms: A router crashes after you have manually configured 237 IPv6 tunnels.

Conditions: This symptom is observed on a Cisco platform that is configured for IPv6 when there are more than eight paths for one IPv6 prefix. The symptom is platform-independent and not release-specific.

Workaround: There is no workaround.

- CSCeh49892

Symptoms: The following incorrect error message is generated when an invalid QOS policy is applied to an L2 ATM interface before a valid policy is applied:

`Remove existing Service-policy CBR before applying new Service-policy egress`

Conditions: This symptom is observed only on a Cisco router that is configured with a secondary RP and ATM L2VPNs that function in the VP mode.

Workaround: There is no workaround.

- CSCeh50638

Symptoms: A 4-port Gigabit Ethernet ISE line card may crash.

Conditions: This symptom is observed on a Cisco 12000 series that is configured for multicast traffic.

Workaround: There is no workaround.

- CSCeh60368

Symptoms: On a Cisco 10000 series that is configured with 6-port channelized T3 line cards, when the primary and standby PREs are each loaded with a different Cisco IOS software release (for example, Release 12.0(28)S and Release 12.0(28)S3) and when the standby PRE boots, the standby PRE may crash or other errors may occur while the standby PRE configures the channelized T3 channels.

Conditions: This symptom is observed on a Cisco 10000 series for Cisco IOS Release 12.0(27)S, Release 12.0(28)S, Release 12.0(30)S, Release 12.0(31)S or a rebuild of these releases when the standby PRE runs a Cisco IOS software release that is either older or newer than the software release on the primary PRE and when one PRE runs a software release that includes the fix for caveat CSCsa41907 and the other PRE runs a software release that does not contain the fix for caveat CSCsa41907.

Workaround: Do not perform live software upgrades. Rather, bring the primary PRE down and boot the standby PRE with the same Cisco IOS software release that runs on the primary PRE, so that when both PREs come up, their software releases match.

Otherwise, upgrade to an image containing the fix for CSCeh60368.

Further Problem Description: When both the primary and standby PRE run a Cisco IOS software release that contains the fix for caveat CSCsa41907, the symptom does not occur.

- CSCeh78918

Symptoms: When a line card has reloaded because you reloaded the router, the line card crashed, or you entered a command to reload the line card, the following message may appear on the console:

`%MDS-2-RP: MDFS is disabled on some line card(s). Use "show ip mds stats linecard" to view status and "clear ip mds linecard" to reset.`

This message may be generated because MDFS is erroneously disabled on the reloaded line card. Erroneous disabling of MDFS may unnecessarily extend network convergence time.

Conditions: This symptom is observed on a distributed router or switch such as a Cisco Catalyst 6000 series, Cisco 7500 series, Cisco 7600 series, Cisco 10000 series, and Cisco 12000 series. The symptom occurs when the router has the **ip multicast-routing distributed** command enabled for any VRF and when a line card is reloaded more than 50 seconds into the 60-second MDFS flow-control period.

Workaround: The symptom corrects itself after 60 seconds. Alternatively, you can enter the **clear ip mds linecard slot number** command.

- CSCei01644

Symptoms: A 3-port Gigabit Ethernet (3GE-GBIC-SC) line card that is configured for Fast-Path Multicast Forwarding may reset when receiving specific packets. However, it is not necessary that the line card will crash all times. The resulting action on these packets could result in a simple drop as well.

Conditions: This symptom is observed on a Cisco 12000 series when a packet with an IP destination address from the reserved multicast range (224.0.0.xxx) and a TTL larger than 1 is received on the 3GE-GBIC-SC line card and when multicast hardware acceleration is enabled.

Normally, the TTL should be 1 if the destination address is part of the reserved multicast range.

Workaround: Enter the **no hw-module slot *slot-number* ip multicast hw-accelerate source-table size 16 offset 0** command.

- CSCei04350

Symptoms: MVPN PIM neighbors that are associated with both a 1-port channelized OC-48 ISE line card and a 1-port channelized OC-12 (DS1) ISE line card bounce when you perform a microcode-reload of a 1-port channelized OC-12 (DS1) ISE line card.

Conditions: This symptom is observed on a Cisco 12000 series.

Workaround: There is no workaround.

- CSCei07556

Symptoms: The PPP protocols flap on a 64K-port of an interface of a 1-port channelized OC-12/STM-4 (DS1/E1) ISE line card that is configured for CoS and that is congested.

Conditions: This symptom is observed when two Cisco 12000 series are connected back-to-back, when the routers are connected via 1-port channelized OC-12/STM-4 (DS1/E1) ISE line cards, and when you send real-time traffic.

Workaround: Change the QoS output policy to prevent traffic from being for longer than 10 seconds and enable keepalive packets to time out.

Further Problem Description: The symptom does not occur when you do not send real-time traffic.

- CSCei07805

Symptoms: When a router has a large VRF configuration and a lot of routing information, the following error messages may be generated during an SSO switchover:

```
%FIB-3-FIBDISABLE: Fatal error, slot/cpu 5/0: keepalive failure
```

The following CPUHOG error message and traceback may also be generated:

```
%SYS-3-CPUHOG: Task is running for (2000)msecs, more than (2000) msecs
(272/145),process = IPC LC Message Handler.
-Traceback= 40EAF5D8 411DBE94 411DBFB8 411DC5D0 411DEFEC 411DEE90 411E0200 41093100
410932B8
```

After the FIBDISABLE error messages has been generated, the router may no longer function properly.

Conditions: This symptom is observed on a Cisco 7600 series but is platform-independent.

Workaround: There is no workaround.

- CSCei07946

Symptoms: When the active rate for a destination PE router is evenly distributed at 4 pps for 20 flows and the active rate for a destination CE router is evenly distributed at 4 pps for 19 flows, one flow is reported at twice that rate (that is, 8 pps).

Conditions: This symptom is observed on a Cisco 12000 series that functions in a MVPN VRF-Lite environment with 20 multicast streams that have a single sustained cell rate (SCR) and that have the pps rate evenly distributed across all streams.

Workaround: There is no workaround.

- CSCei15701

Symptoms: The active PRP pauses indefinitely after it changes from standby to active.

Conditions: This symptom is observed when the redundant PRPs are configured for RPR+ mode, the router has two APS-protected CHOC12 line cards, the router has mVPNs configured, and the router runs Cisco IOS Release 12.0(28)S3.

Workaround: There is no workaround.

- CSCei19563

Symptoms: A faulty PRE may unexpectedly switch from standby mode to active mode, causing the active PRE to crash.

Conditions: This symptom is observed on a Cisco 10000 series that has dual PREs and that runs Cisco IOS Release 12.0(25)SX6 but may also occur in Release 12.0S.

Workaround: Remove the faulty PRE.

- CSCei22697

Symptoms: Some MVPN tunnels are mapped to an incorrect VRF forwarding table.

Conditions: This symptom is observed on a Cisco router that is configured for data MDT groups.

Workaround: There is no workaround.

- CSCei35132

Symptoms: When a link failure occurs between two provider (P) routers, the LSP that is protected via Fast Reroute (FRR) for a primary tunnel and the directed LDP session within the tunnel are fast-rerouted onto an assigned backup tunnel. However, when the backup tunnel goes down, VPN prefixes that are protected by backup TE LSP entries in the LFIB become "Untagged." This situation causes packet loss for ATOM and L3VPN traffic that uses the link between the P routers as its primary path.

Conditions: These symptoms are observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S, that functions as a P router, and that is connected to another P router via a 4-port OC-3 ISE line card.

The topology is as follows:

PE ----- P --- OC-3 --- P ----- PE

There are one-hop primary tunnels between every pair of routers that is listed above, and each link is protected by an NHOP backup tunnel LSP.

The symptom occurs when you pull the TX fiber cable from the 4-port OC-3 ISE line card that forms the protected link between the two P routers, when the protected LSP is fast-rerouted onto the backup tunnel, and when the backup tunnel is torn down. One P router may show "Untagged" entries in its LFIB, especially for a loopback interface to a provider edge (PE) router. This situation breaks the forwarding for all of the L2 and L3 VPNs that depend on that PE router.

The symptom is timing-dependent. The symptom does not occur all the time and does not seem to be Cisco 12000 series line card-dependent, nor is it specific to a link between the two P router because the symptom may also occur when you pull the TX fiber cable of a line card that forms the link between a PE router and a P router.

Workaround: There is no workaround.

- CSCei36381
Symptoms: When QOS parameters are changed, traffic does not pass via an L2TPv3 link.
Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S when QOS or HQoS parameters are changed and affect the traffic flow.
Workaround: Reload the affected line card or reload the router.
- CSCei38116
Symptoms: ISE line cards crash when a Cisco 12000 series receives 640,000 multicast streams.
Conditions: This symptom is observed when the memory of the ISE line cards becomes exhausted when the thousands of multicast streams are received.
Workaround: There is no workaround.
- CSCei40168
Symptoms: An AToM VC that is configured on a Fast Ethernet or Gigabit Ethernet interface may not be functional and packets that are received on the interface are dropped.
Conditions: This symptom is observed on a Cisco 10720.
Workaround: Reconfigure the **xconnect** command on the affected interface.
Further Problem Description: When the symptom occurs, the output of the **show hardware pxf cpu statistics interface interface-name detail** command shows that the packets that are received on the interface are dropped because of an “mpls undefined port” condition.
- CSCei40439
Symptoms: The output of the **show policy-map interface** command for an interface that is configured for Weighted Random Early Detection (WRED) is not correct. The traffic details in the command output should be displayed with respect to the class maps but are not.
Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.0(28)S3.
Workaround: There is no workaround.
- CSCei43961
Symptoms: When you ping between two CE routers, the connected PE router does not show the appropriate entry in the NetFlow table.
Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.0(30)S3, that is configured with a PRE1, and that functions as a PE router when the **mpls netflow egress** command is enabled.
Workaround: There is no workaround. Note that the symptom does not occur in Release 12.0(24)S6.
- CSCei48972
Symptoms: After a manual switchover occurs in RPR+ mode, a VPN that is configured on a Frame Relay subinterface fails to recover and CEF may be disabled on line cards.
Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of a Cisco IOS interim release for Release 12.0(30)S2.
Workaround: Enter the **hw-module slot slot-number reload** command.
- CSCei54336
Symptoms: An MPLS LER does not impose labels for traffic that follows the default route, causing traffic to be forwarded via IP.

Conditions: This symptom is observed on a Cisco 12000 series when the default route has two equal paths, when the ingress line card is an ISE line card, and when the default router is learned via OSPF. The symptom may also occur for other protocols.

Workaround: Use a single path for the default route. If this is not an option, there is no workaround.

- CSCei55626

Symptoms: When two routers are configured for Multi-Router APS (MR-APS) and when a forced switchover occurs, MLP interfaces on the router with the inactive APS interface stay up and traffic leaves via the inactive APS interface rather than via the active APS interface.

Conditions: This symptom is observed when two Cisco 10000 series routers are configured for MR-APS and connected via channelized OC-3 line cards.

Workaround: There is no workaround.

- CSCei61732

Cisco IOS may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.

Cisco has made free software available that includes the additional integrity checks for affected customers.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml>.

- CSCei75919

Symptoms: High CPU use may occur on line cards and may cause instability in control plane protocols.

Conditions: This symptom is observed on a Cisco 12000 series that functions in a mVPN decapsulation environment with core-facing Engine 4+ line cards and ISE line cards that are configured with VRFs and for hardware forwarding.

Workaround: There is no workaround.

- CSCei83644

Symptoms: A nondefault configuration becomes lost for a serial interface on a channelized OC-48 ISE line card or on a 4-port OC-12 ISE line card.

Conditions: This symptom is observed on a Cisco 12000 series after you have reloaded the router.

Workaround: There is no workaround.

- CSCei87923

Symptoms: A policy on a main Ethernet interface does not properly match packets for one of its subinterfaces.

Conditions: This symptom is observed on a Cisco 12000 series Ethernet ISE line card when one of its subinterfaces is configured for Xconnect and has a layer 2 VPN configured and when the following events occur:

- You attach a policy to the subinterface.
- You remove the policy from the subinterface.
- You attach the policy to the main interface.

Workaround: There is no workaround.

- CSCei90536

Symptoms: mVPN packets have corrupted encapsulation headers.

Conditions: This symptom is observed on a Cisco 12000 series that has a channelized ISE ingress line card when packets are replicated to a VRF interface on the ingress line card, to a VRF interface on another line card, and to a core interface on a third line card. This symptom occurs only after some redundancy switchovers.

Workaround: Reload the line card.

- CSCei90588

Symptoms: A bad checksum error, bad LLS TV length error, or both are reported on a router that is configured for OSPF and BGP. These protocols or other configured protocols may flap during the errors, and data packets that are sent to the RP may be lost.

Conditions: These symptoms are observed on a Cisco router when the following conditions are present:

- OSPF, BGP, and other control protocols are configured with scaled routes and peers.
- Congestion occurs on the RP because of the control packets that are targeted to the RP in the router. Also, if additional traffic is sent to one of the IP addresses of the router, the packets are terminated on the RP. For example, IP ping packets that are directed towards one of the loopback addresses are terminated on the RP.

Workaround: There is no workaround.

- CSCej01743

Symptoms: Traffic drops may occur when traffic is sent over MFR or Frame Relay links.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S1 or a later release and that is configured for software forwarding.

Workaround: There is no workaround.

- CSCej12324

Symptoms: A Cisco 10000 series drops a packet for a prefix with an incomplete CEF adjacency.

Conditions: This symptom is observed when the PXF engine does not punt the packet with the incomplete CEF adjacency to the RP (as it is supposed to do) but drops the packet.

Workaround: Send a ping for the prefix with the incomplete CEF adjacency in order to complete the CEF adjacency.

- CSCej15682

Symptoms: When multicast traffic is being sourced from different sources, and one of the sources is removed, the **show ip mroute vrf** command for the VRFs still shows that source as active.

Conditions: This symptom is observed when a source is no longer active when using the **show ip mroute vrf** command.

Workaround: There is no workaround.

- CSCej22910

Symptoms: Multicast traffic does not reach a CE which is connected via static IGMP joins to PE.

Conditions: The DecapPE should have a Tx line card with one port toward the core and another port toward the edge. Traffic from EncapPE is toward the CE. There should be static joins at DecapPE with SSM configured.

Workaround: There is no workaround.

- CSCej26744

Symptoms: The **show policy-map** command on the POS E3 and E6 interface is not working properly.

Conditions: This symptom is observed when applying policy with confirm and exceed conditions and then executing the **show policy- map** command.

Workaround: There is no workaround.

- CSCej28374

Symptoms: Tracebacks were observed when applying a service policy to a main interface if a subinterface is configured. The subinterface inherits the service policy, producing the tracebacks. There was no adverse behavior of the service policy. It worked properly but triggered tracebacks.

Conditions: The tracebacks could be observed if the configuration includes subinterfaces and if a service policy is applied to the main interface.

Workaround: Remove the service policy on the main interface and apply it to the subinterface in the configuration.

- CSCin72437

Symptoms: A port adapter in a router or FlexWan module in a switch may crash when an SSO switchover occurs on a Route Processor or Supervisor Engine.

Conditions: This symptom is observed when the port adapter or FlexWan module is configured with a QoS policy.

Workaround: There is no workaround.

- CSCin79691

Symptoms: QoS information disappears from a FlexWAN module or VIP that is configured with a distributed MFR interface.

Conditions: This symptom is observed after the FlexWAN module or VIP resets or after the interface flaps.

Workaround: Remove the service policy from the interface and reapply it to the interface.

- CSCsa64476

Symptoms: A Cisco 10000 series generates the following error message:

```
%GENERAL-3-EREVENT: ACLs could not add IDB to list
```

The message is followed by a traceback.

This may indicate that the standby PRE does not apply the ACL for security purposes.

Conditions: This symptom is observed on a Cisco 10000 series that is configured with redundant PREs. The symptom is a timing issue.

Workaround: There is no workaround.

- CSCsa65096

Symptoms: A router may crash during the boot process when the startup configuration includes the **hw-module shutdown** command.

Conditions: This symptom is observed on a Cisco 10000 series but is platform-independent. A list of the affected releases can be found at

<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsa51602>. Cisco IOS software releases not listed in the “First Fixed-in Version” field at this location are not affected.

Workaround: There is no workaround.

- CSCsa77411

Symptoms: A crash that is related to MPLS TE bandwidth management may occur on a Cisco router which is configured for OSPF and MPLS Traffic Engineering.

Conditions: This symptom is observed on a Cisco router that integrates the fix for caveat CSCef16096 when the following conditions are present:

- The router is configured for OSPF and MPLS traffic engineering (TE).
- The interfaces, OSPF adjacencies, and TE tunnels are flapping.
- There are more than 300 OSPF interfaces (in any state, including administratively down) in the OSPF area that is configured for MPLS TE.

You can check the number of interfaces by entering the **show ip ospf** or **show ip ospf interface brief** command. Note that all interfaces that are covered by network statements are included in the command output, even those that are in the administratively down state.

A list of the affected releases can be found at

<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCef16096>. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

Workaround: There is no workaround.

- CSCsa84587

Symptoms: A 6PE router crashes during an IPv6 ping to another PE router at the far side of the network.

Conditions: This symptom is observed when you enter the **no mpls ipv6 source-interface** command followed by **no interface type number** command in which the *type number* argument represents the IPv6 source interface that was configured in the **mpls ipv6 source-interface** command.

Workaround: When you want to disable the IPv6 source interface, first enter the **no interface type number** command in which the *type number* argument represents the IPv6 source interface that is configured in the **mpls ipv6 source-interface** command and then enter the **no mpls ipv6 source-interface** command.

- CSCsa88340

Symptoms: Unicast traffic that travels over an ATM subinterface between a PE router and a CE router stops.

Conditions: This symptom is observed on a Cisco 12000 series that functions as a PE router and that is configured with an ATM ISE line card when the following conditions are present:

- Remove the VRF that has only the ATM subinterface associated to it.
- Define a new VRF and remap the ATM subinterface to this new VRF.
- Enable RPF on the ATM subinterface.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the ATM subinterface or remove and re-add the ATM subinterface configuration.

- CSCsb05218

Symptoms: An IPv6 ACL configuration may be lost or incorrect after an SSO switchover.

Conditions: This symptom is observed when a Cisco 12000 series performs IPv6 ACL filtering and when the ACL is modified.

Workaround: There is no workaround.

- CSCsb14703

Symptoms: The PXF engine of a Cisco 10000 series crashes.

Conditions: This symptom is observed when a Fast Ethernet port flaps because you change the duplex configuration.

Workaround: Do not change the duplex mode.

- CSCsb18880

Symptoms: A 4-port channelized STM-1/OC-3 line card resets and generates an “IRONBUS-FAULT” error message.

Conditions: This symptom is observed on a Cisco 10000 series when you enter the **tug-2 tug-2-number e1 e1-number loopback** command on the line card.

Workaround: There is no workaround.

- CSCsb27311

Symptoms: After you have send linerate traffic via an IMA interface for a while, a ping fails in a packed cell relay configuration via ATM over L2TPv3 pseudowires.

Conditions: This symptom is observed in a scalable packed cell relay configuration on an IMA interface of a PA-A3-8E1IMA or PA-A3-8T1IMA port adapter that is installed in a Cisco 7200 series or Cisco 7500 series.

Workaround: There is no workaround.

- CSCsb29326

Symptoms: An snmpwalk for cmplsFrrFacObjects for the FRR-MIB fails to show entries for a tunnel headend.

Conditions: The symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(26)S6, Release 12.0(28)S3, or Release 12.0(31)S.

Workaround: There is no workaround.

- CSCsb33258

Symptoms: An RP crashes during BGP convergence when MVPNs are configured.

Conditions: This symptom is observed on a Cisco router after a duplicate BGP MDT extended community message is received that specifies a different Route Descriptor (RD) for an MDT that already exists for the specified MDT source and group address.

Workaround: There is no workaround.

- CSCsb41367

Symptoms: When you enter the **redundancy force-switchover** command, an Engine 4 line card may crash.

Conditions: This symptom is observed on a Cisco 12000 series that runs the c12kprp-p-mz Cisco IOS software image and that has two RPs that function in SSO mode.

Workaround: There is no workaround.

- CSCsb53420

Symptoms: Cell loss occurs when bursty VBR ATM traffic is sent through a Cisco 12000 series 4-port ATM OC-12 ISE line card via an L2TPv3 IP tunnel to another 4-port ATM OC-12 ISE line card on another Cisco 12000 series and when the VBR traffic is sent at rates lower than what is configured on the routers (that is, at about 50 percent of the OC-12 line rate).

Conditions: These symptoms are observed on a Cisco 12000 series that is connected back-to-back via an OC-192 or OC-48 POS link to another Cisco 12000 series.

Workaround: There is no workaround.

- CSCsb54190

Symptoms: When you shut down an SRP interface on which the egress L2 priority is set to high by entering the **no shutdown** interface configuration command, the PXF engine of a downstream router may crash.

Conditions: This symptom is observed on a Cisco 10720.

Workaround: Do not enter the **no shutdown** interface configuration command. Rather, force a ring wrap by entering the **srp ips forced-switch** command.

- CSCsb59294

Symptoms: The output is stuck on a Cisco 7200 series.

Conditions: This symptom is observed when a service policy attached to a T1 or E1 ingress interface on one of the following port adapters:

- PA-MC-2T1
- PA-MC-2E1/120
- PA-MC-4T1
- PA-MC-8T1
- PA-MC-8E1/120
- PA-MC-8TE1+

Workaround: Remove the service policy from the egress interface.

- CSCsb62041

Symptoms: A newly created channelized interface may show packet and byte counts before any traffic passes through the interface.

Conditions: This symptom is observed on a Cisco 12000 series. When a channelized interface is deleted, the interface index is released. This interface index may be re-allocated when a new channelized interface is created. The counters that are associated with the index need to be cleared when an interface is deleted so that they are properly initialized if the index is subsequently re-allocated to a new interface.

Workaround: There is no workaround. Although you can clear the interface counters via the CLI, doing so does not prevent the symptom from occurring because but there is an internal counter that is used in the Tx byte and packet counts and that may cause errors in the calculations.

- CSCsb75433

Symptoms: Distributed Multilink PPP (dMLP) packets are not switched via dCEF.

Conditions: This symptom is observed on a Cisco router that is configured with multilink bundles.

Workaround: There is no workaround.

- CSCsb93720

Symptoms: Using “no <any config CLI>” command may not get synchronized to standby RP. After switchover, the interface shows configuration still enabled.

Conditions: This symptom is observed on a Cisco 12000 series router that is running the c12kprp-p-mz/grs-p-mz image of Cisco IOS Releases 12.0(30)S and 12.0(31)S.

Workaround: Reconfigure “no <any config CLI>” command after switchover.

Wide-Area Networking

- CSCef54653

Symptoms: Some members of a multilink bundle remain inactive, while others are active.

Conditions: This symptom is observed when the interfaces are configured with the **ppp chap hostname** or **ppp multilink endpoint** command. Very high speed interfaces may come up and join the multilink bundle faster than the configuration can be processed, which causes them to use the host name of the router (instead of the configured user name or endpoint value) as the Endpoint Discriminator during Link Control Protocol (LCP) negotiations. This situation causes a mismatch between these links and those that come up after the configuration command is processed.

Workaround: Enter the **shutdown** interface configuration command followed by **no shutdown** interface configuration command on the active links to enable the links to renegotiate LCP with the correct Endpoint Discriminator value.

- CSCeg88737

Symptoms: A Cisco 7200 series may crash because of memory corruption.

Conditions: This symptom is observed when the router has an input QoS configuration on an MFR interface.

Workaround: There is no workaround.

- CSCsa87205

Symptoms: A router that is configured for PPP Multilink reloads because of a bus error.

Conditions: This symptom is observed after a Telnet or SSH session is established when you enter the **who** command.

Workarounds: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.0(30)S3

Cisco IOS Release 12.0(30)S3 is a rebuild of Cisco IOS Release 12.0(30)S. The caveats listed in this section are resolved in Cisco IOS Release 12.0(30)S3 but may be open in previous Cisco IOS releases. This section describes only severity 1, severity 2, and select severity 3 caveats.

Basic System Services

- CSCed44414

Symptoms: When the slave RSP crashes, a QAERROR is observed in the master console, resulting in a cbus complex. The cbus complex will reload all the VIPs in the router.

Conditions: This symptom happens when the slave crashes in a period when there is a large number of packets going towards the RSP. A large number of packets go to the RSP when CEF switching is configured or when routing protocol updates are numerous.

Workaround: There is no workaround.

- CSCeg16078

Symptoms: You cannot create a VRF-aware ICMP, UDP, or jitter probe using SNMP.

Symptoms: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.0(27)S. Note that the symptom does not occur in Release 12.2(11)T.

Workaround: Use CLI commands to create a probe.

- CSCeg41734

Symptoms: The console of a router may stop responding and the router may stop forwarding traffic.

Conditions: This symptom is observed on a Cisco 7206VXR that runs Cisco IOS Release 12.3(6b) and that is configured with an NPE-G1 when the native Gigabit Ethernet interfaces of the NPE-G1 are used. The symptom may also occur in other releases.

Workaround: There is no workaround.

- CSCuk51587

Symptoms: The following error message is generated when you insert a VIP into a previously empty slot of a Cisco 7500 series.

```
%COMMON_FIB-2-HW_IF_INDEX_ILLEGAL: Attempt to create CEF interface for unknown if  
with illegal index: 0
```

Conditions: This symptom is observed on a Cisco 7500 series that is configured for CEF.

Workaround: There is no workaround.

Interfaces and Bridging

- CSCef01220

Symptoms: A Versatile Interface Processors (VIP) with a PA-MC-8TE1 port adapter may report its memory size as unknown even though the VIP appears to function normally, and Distributed Multicast Fast Switching (DMFS) may fail to function properly.

Conditions: This symptom is observed on a Cisco 7500 series when any of the following conditions are present:

- The mode of the controller of the PA-MC-8TE1 port adapter is not set to T1 or E1 and you insert or remove another VIP with any port adapter via an OIR.
- Irrespective of whether or not the mode of the controller of the PA-MC-8TE1 port adapter is set to T1 or E1, you insert or remove a standby RSP via an OIR.

Workaround: Enter the **card type {t1 | e1} slot [bay]** command on the PA-MC-8TE1+ port adapter and ensure that none of the controllers on this port adapter are shut down.

- CSCin88718

Symptoms: All channels on a PA-MC-2T3+ port adaptor stop sending traffic although they continue to receive packets. All interfaces will remain in up/down state.

Conditions: Once we send greater than linerate over the port adaptor, for a little while the PA locks up and never returns to normal working state.

Workaround: Perform resurrect operation on the PA. Note: this will affect all interfaces on that PA.

- CSCsa87986

Symptoms: A router may intermittently transmit corrupt PPP packets. When you enter the **debug ppp nego** and **debug ppp errors** commands, it appears that “protocol reject” packets are received from the remote end.

Conditions: This symptom is observed on a Cisco 7500 series that has only one OC3 POS port adaptor per VIP and that is configured for PPP encapsulation.

Workaround: There is no workaround.

IP Routing Protocols

- CSCef95026

Symptoms: When interfaces flap, a Cisco router may reload unexpectedly because of a bus error.

Conditions: This symptom is observed when OSPF accesses a freed LSDB entry.

Workaround: There is no workaround.
- CSCeg07725

Symptoms: A router may continue to redistribute an eBGP route into EIGRP after the eBGP route is deleted or EIGRP may not redistribute an eBGP route after the eBGP route has been installed.

Conditions: This symptom is observed on a Cisco router that redistributes eBGP routes into EIGRP when the router functions in a multihoming environment.

The symptom occurs in a configuration with two PE routers that advertise routes via eBGP and a border router that is configured with a higher local preference than the PE routers when the eBGP route of the primary path is withdrawn and the route of the secondary path is installed.

Workaround: If a route is still redistributed into EIGRP after the eBGP route is deleted, clear the BGP peer from which the eBGP route used to be learned so EIGRP stops advertising the route.

If a route is not redistributed into EIGRP after an eBGP route is installed, clear the route so EIGRP starts advertising it. Another workaround is to enter the **bgp redistribute-internal** command to cause EIGRP to redistribute iBGP routes and to prevent EIGRP from failing to redistribute an updated BGP route.
- CSCeg54375

Symptoms: Routing inconsistencies may occur in the RIB: routes may be missing from the RIB but may be present in the BGP table.

Conditions: This symptom is observed on a Cisco RPM-XF when the toaster processor crashes. However, the symptom may occur on any platform that has a toaster processor.

Workaround: Enter the **clear ip route vrf vrf-name *** command.
- CSCeg89700

Symptoms: A Cisco router does not recognize an end-of-RIB message from a third-party vendor router and continues to show the “Neighbor is currently in NSF mode” message although the restart procedure of the third-party vendor router is complete.

Conditions: This symptom is observed on a Cisco router that is configured for IPv6 BGP peering and NSF. Note that the symptom does not occur when IPv4 BGP peering is configured.

Workaround: There is no workaround.
- CSCeh16989

Symptoms: The Multiprotocol BGP (MP-BGP) network entries counter increases above the real number of reachable networks.

Conditions: This symptom is observed when network activity occurs in a non-converged environment. The correct number of network entries is restored when there is a period of BGP stability that last for about 1 minute or more because BGP is able to converge and the scanner has time to run and collect the old network entries. However, if there is a sustained period of churn and BGP is only able to converge for a few seconds before new updates arrive, old BGP network entries are not cleaned up, causing the MP-BGP network entries counter to increase above the real number of reachable networks.

Workaround: There is no workaround.

- CSCeh33504

Symptoms: A router terminates 102,000 VPNv4 routes but route reflectors (RRs) report only a subset of the total.

Conditions: This symptom is observed on a Cisco MGX RPM-XF that runs Cisco IOS Release 12.3(11)T4 when 204 routes are configured per VRF over 496 VPNs (one VPN has about 1000 routes). However, Cisco MGX RPM-PRs that function as RRs show that only 76245 routes are terminated on the Cisco MGX RPM-XF. The symptom may be platform-independent.

Workaround: There is no workaround.

- CSCsa57101

Symptoms: A Cisco router may reload when the RSVP MIB object is polled via SNMP.

Conditions: The symptom is platform- and release-independent.

Workaround: Disable SNMP by entering the **no snmp-server host** command.

- CSCsa87473

Symptoms: A BGP speaker may fail to send all of its prefixes to a neighbor if the neighbor sends a refresh request to the BGP speaker at the same time that the BGP speaker is generating updates to the neighbor. This situation causes the neighbor to miss some prefixes from its BGP table.

Conditions: This symptom may occur between any pair of BGP speakers.

A common scenario is that a VPNv4 PE router is reloaded and then fails to learn all prefixes from its route reflector (RR). In this configuration, the symptom occurs when the processing of a VRF configuration causes the PE router to automatically generate a route-refresh request to the RR, while the RR is still generating updates to the PE.

Workaround: There is no workaround.

ISO CLNS

- CSCsb07279

Symptoms: When an IPv4 prefix list is used in a redistribution command for the IS-IS router process, a change in the prefix list is not immediately reflected in the routing tables of a router and its neighbor. The change may take up to 15 minutes to take effect.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(28)S.

Workaround: To have a change take effect immediately, enter the **no redistribute route-map** command followed by the **redistribute route-map** command for the IS-IS router process.

Miscellaneous

- CSCdz21768

Symptoms: The **show interfaces** and **show ip interface brief** commands may not list interfaces in the expected order.

Conditions: This symptom is observed after channelized interfaces have been removed and added.

Workaround: Reload microcode onto the affected line card.

- CSCec25942

Symptoms: A POS Engine 2 line card originates a high traffic volume to a downstream router over a POS link because the same packet is sent over and over.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(22)S5.

Workaround: There is no workaround.

- CSCed57204

Symptoms: When a large number of VRFs are configured, input OAM F5 loopback cells on the ATM interface are dropped continuously, even without traffic. You can see drops at “OAM cell drops” in the output of the **show atm traffic EXEC** command and at “Input queue drops” in the output of the **show interface ATM EXEC** command.

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.2(19), Release 12.3(5), or Release 12.3(4)T2 when the **oam-pvc manage** and **ip vrf** global configuration commands are configured. The symptom may also occur in other releases.

Workaround: Remove the **ip vrf** command. There is no workaround for a router such as a provider edge (PE) router that cannot remove VRFs.

- CSCee04893

Symptoms: A Cisco router is not able to forward traffic to a TE tunnel.

Conditions: This symptom has been observed on a Cisco 10000 running Cisco IOS Release 12.0(26)S1 and Release 12.0(27.3)S1 with Multilink PPP + MPLS + TE Tunnel.

Workaround: There is no workaround.

- CSCee43853

Symptoms: The following tracebacks are generated when a Cisco 10000 series is reloaded or when a manual or unexpected PRE switchover occurs:

```
%FIB-2-HW_IF_INDEX_ILLEGAL: Attempt to create CEF interface for unknown if with
illegal index: 0
-Traceback= 602FF2F0 603061EC 6040257C 60099DD4 60099F20 6009A574 604D8E88604E0040
603C85C8 603D80CC 603D8310 6048381C 6047EEC4 6047894C 60480EF4 604810CC
```

Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.0(30)S or Release 12.0(30)S1 and occurs always when Gigabit Ethernet line cards are installed in the router. The occurrence of the symptom does not depend on any other particular configuration of the router, and the tracebacks are generated only at startup, not during normal operation.

Workaround: There is no workaround.

- CSCee49035

Symptoms: An incorrect update-source interface is selected for a multicast tunnel interface in an MVPN configuration.

Conditions: This symptom is observed when the provider edge (PE) router is also an ASBR with eBGP peers or has non-VPNv4 peers with higher IP addresses than the peer that has VPNv4 enabled. MVPN requires that the BGP update source address of a VPNv4 peer is selected as the MTI source address.

Workaround: There is no workaround.

- CSCef23912

Symptoms: A traceback is generated on the console and logged in the logging buffer, and the count in the output of the **show alignment** command increments.

Conditions: This symptom is observed on a Cisco 10000 series that is configured as a provider edge (PE) router when you enter the **show mpls forwarding** command to show the pop labels and the active LDP peers.

Workaround: There is no workaround.

- CSCef25686

Symptoms: A number of PVCs may become locked in an inactive state, and the following type of error message may appear in the log:

```
%ATM-3-FAILREMOVEVC: ATM failed to remove VC(VCD=X, VPI=X, VCI=X) on Interface ATM X/X/X,
```

```
(Cause of the failure: PVC removal during recreation failed)
```

Conditions: This symptom is observed when you change the parameters of a VC class while the PVC is active and while you view the PVC status in the output of the **show atm vc interface interface-number** command.

The symptom occurs when you change the PVC speed in a VC class via one Telnet (or console) session and you enter the **show atm vc interface interface-number** command via another Telnet (or console) session.

Workaround: To remotely resolve the symptoms, remotely initiate an HA failover or remotely reload the affected router.

- CSCef41934

Symptoms: A router processes incoming LSP ping packets as unlabeled IP packets on a VRF interface or a non-MPLS interface.

Conditions: This symptom is observed on a Cisco router that has the MPLS LSP Ping feature enabled.

Workaround: Use an ACL to block port 3503 that is used for LSP ping packets. However, note that this may prevent some MPLS LSP Ping applications from functioning properly, as noted below:

LSP ping packets that enter on a VRF interface are dropped because the router uses the global routing table in its attempt to reply to MPLS echo requests, which could cause the reply to be forwarded to the wrong destination.

LSP ping packets that enter on an interface that is not configured for MPLS are processed, but depending on the type of MPLS echo packet, the following occurs:

- MPLS echo request packets are dropped.
- MPLS echo reply packets are not dropped. (It possible for an MPLS echo reply packets to be received on a non-MPLS interface because the reply path is asymmetric with the forward LSP.)

- CSCef50208

Symptoms: The number of transmitted broadcast packets is not shown in the **show interface** command on Ethernet interfaces. The customer needs to see this counter in the **show interface** command, just like the number of received broadcasts.

Conditions: The feature is implemented only for Ethernet interfaces on GSR platforms.

Workaround: There is no workaround.

- CSCef59507

Symptoms: A failed LDP session may still show up in the output of the **show mpls ldp neighbors** command as well as the new working session after the neighborship is re-established. The display of two sessions, one not working and one working to the same neighbor, may mislead the MPLS network operator.

Conditions: This symptom may occur after an LDP session has gone down and then re-established.

Workaround: There is no workaround.

- CSCef64439

Symptoms: A PRE requires a long time to enter the STANDBY HOT state after a switchover.

Conditions: This symptom is observed on a Cisco 10000 series when two PREs are forced to switchover back and forth.

Workaround: Enter the **snmp-server ifindex persist** command.
- CSCef79749

Symptoms: APS does not function correctly on a channelized OC-48 ISE line card and the output of the **show aps** command shows that the line card is down.

Conditions: This symptom is observed on a Cisco 12000 series.

Workaround: There is no workaround.
- CSCef87449

Symptoms: After **shutdown** of the outgoing interface of a TE LSP, the Resv state should be removed immediately. However, the Resv state will remain in place until a PathTear arrives or a timeout causes state teardown.

When the TE headend is running Cisco IOS, the Path Tear is sent very quickly and the state is removed.

This symptom is short-lived and it is very unlikely to be noticed.

Conditions: The Cisco IOS router must be running an image with the fix for CSCec26563 and have MPLS Traffic Engineering tunnels enabled.

Workaround: There is no workaround.
- CSCeg13599

Symptoms: If PGP communication fails on a Cisco 12000 router configured with MR-APS, then both APS interfaces can end up in Active state. This situation does not get corrected automatically and manual intervention is required to correct the situation. This can result in traffic duplication in the ingress direction.

Conditions: This symptom affects Cisco IOS Release 12.0(30)S for the Cisco 12000 platform. Other platforms and releases are not affected. The PGP failure should happen when the Protect is in Active state.

Workaround: There is no workaround.
- CSCeg21025

Symptoms: In a multirouter-automatic protection switching (MR-APS) configuration involving Cisco 12000 routers and OC3 or OC12 ATM ISE line cards, both interfaces participating in MR-APS transition to Inactive state. This is a software inconsistency and can result in traffic loss.

Conditions: After the following set of steps, both of the MR-APS interfaces end up in Inactive state. This symptom happens in a scaled configuration of about 1000 VCs.

 1. Protect is Active, Working is Inactive.
 2. Working member is unconfigured.
 3. Switch from Protect to Working.
 4. Reconfigure working member.

Workaround: There is no workaround.

- CSCeg35517

Symptoms: An Engine 3 1-port OC-12 channelized DS1 line card that is configured for MLP may reset or may cause the RP to reset.

Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of Cisco IOS Release 12.0(31)S.

Workaround: There is no workaround.

- CSCeg35670

Symptoms: Shortly after a Cisco IOS software boot loader image has been downloaded, a PRP-2 may crash and does not reload.

Conditions: This symptom is observed on a Cisco 12000 series that runs the boot loader image of Cisco IOS Release 12.0(30)S.

Workaround: There is no workaround.

- CSCeg65439

Symptoms: A Cisco 12000 series may hang while reloading.

Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz or c12kprp-p-mz image of an interim release for Cisco IOS Release 12.0(31)S.

Workaround: There is no workaround.

- CSCeg79456

Symptoms: An Engine 6 line card may reset because of an IPC timeout.

Conditions: This symptom is observed on a Cisco 12816 that runs Cisco IOS Release 12.0(27)S4 when you enter the **shutdown** command on the primary Clock Scheduler Card (CSC) or you enter the **no shutdown** command on the secondary CSC that is in the shut down state.

Workaround: There is no workaround.

- CSCeg83164

Symptoms: A router may reload when you configure an ATM VC class.

Conditions: This symptom is observed on a Cisco 7200 series and Cisco 7500 series that are configured for MPLS but may be platform-independent.

Workaround: There is no workaround.

- CSCeg83614

Symptoms: A router that has MPLS traffic engineering tunnels and that is configured for Fast ReRoute may crash because of memory corruption.

Conditions: This symptom is observed only on a Point of Local Repair when a primary tunnel has bandwidth protection enabled via the **tunnel mpls traffic-eng fast-reroute bw-protect** command and when more than eight LSPs are pre-empted to make room for the bandwidth-protected LSP.

Workaround: There is no workaround.

- CSCeg88655

Symptoms: A RP switchover causes %SYS-2-NOTQ and %SYS-2-LINKED errors and some tracebacks on a Cisco 12000 series 1-port channelized OC-12c/STM-4 (DS1/E1) ISE line card.

Conditions: This symptom is observed on a Cisco 12000 series dual-PRP router that runs a Cisco IOS interim release for Release 12.0(31)S.

Workaround: There is no workaround.

- CSCeg89202

Symptoms: When you attach a policy with a priority class to a subinterface of a channelized OC-48/STM-16 (DS3/E3, OC-3c/STM-1c, OC-12c/STM-4c) POS/SDH ISE line card that is configured with Frame Relay subinterfaces, the default queue limit for the priority queue of the port changes to a value that is calculated by the policy map that was attached. This situation causes QoS to be impacted.

Conditions: This symptom is observed on a Cisco 12000 series.

Workaround: Ensure that the policy map that you attach last calculates the desired queue limit, which is then applied to all subinterfaces of the port.

- CSCeh02579

Symptoms: A multilink bundle on a Cisco 10000 series may lock up. The multilink bundle may transmit packets but does not process any incoming packets, indicating that all links of the bundle are in an out-of-order state and draining.

Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.0(25)SX, Release 12.0(26)S4, or a later 12.0S release and that is configured for mVPN and MLP. The symptom may be platform-independent.

Workaround: If this is an option, disable mVPN.

- CSCeh05751

Symptoms: Hardware multicast may be disabled on an Engine 3 line card and the line card may reset.

Conditions: This symptom is observed when you scale BGP routes and load-balancing on a PE router that is configured for MVPN.

Workaround: There is no workaround.

- CSCeh07851

Symptoms: There are several symptoms:

- Multicast traffic may be punted to the RP with the “no group” reason, even if (*,G) and (S,G) exist on the PXF. You can observe the punted traffic in the output of the **show hardware pxf cpu statistics diversion** command.
- PIM neighbors across an MDT in an MVPN network may flap.

Conditions: This symptom is rarely observed when either PXF or the router is rebooted or reloaded while traffic runs in the network. When the router has a large configuration or when many multicast streams pass through the router, the probability of the symptom occurring increases.

Workaround: Make a note of the traffic streams that are punted to the RP by entering the **show hardware pxf cpu statistics spd** command. Then, clear these traffic streams by entering the **clear ip mroute group** command.

When the multicast routing table is small, just enter the **clear ip mroute *** command.

Further Problem Description: The packets that are punted to the RP are rate-limited by a multicast data traffic SPD process. These packets are counted as “no group”.

In an MVPN network, control plane traffic is encapsulated in an MDT. If this MDT traffic is punted and rate-limited, the control plane traffic is lost, causing PIM neighbors to flap.

- CSCeh12675

Symptoms: Traffic may not fully converge after you have reloaded a line card with a scaled configuration or after an HA switchover.

Conditions: This symptom is observed on a Cisco 12416 that runs the c12kprp-p-mz image of a Cisco IOS interim release for Release 12.0(31)S and that is configured with dual PRPs and a scaled configuration.

Workaround: There is no workaround.

- CSCeh14012

Symptoms: A 1-port channelized OC-12/STM-4 (DS1/E1) ISE line card on a CE router may crash when many (168) MLP interfaces are deleted and reconfigured via TFTP on a directly-connected PE router.

Conditions: This symptom is observed on a Cisco 1200 series that functions as a CE router.

Workaround: There is no workaround.

- CSCeh14063

Symptoms: MPLS Layer 3 VPN traffic cannot be forwarded from a main interface that is also used for Layer 3 VPN de-aggregation traffic and Layer 2 VPN traffic.

Conditions: This symptom is observed on Cisco 12000 series POS ISE line card that is configured for Frame Relay encapsulation when one of its subinterfaces is used for Layer 3 VPN de-aggregation and when a Frame Relay DLCI that is used for Layer 2 VPN traffic is configured on the same main interface.

Workaround: There is no workaround.

- CSCeh15364

Symptoms: On a router that is configured for multi-router APS, the APS interfaces remain in the Active/Inactive states. One of the interfaces is Active, while the other is Inactive. However, when the line card holding the APS protect interface is reloaded and the line card comes back up, both the Working and Protect interfaces end up in Active state.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S2. Not every protect line card reload causes the symptom occur. The symptom is readily observed when the reload of a Protect line card is accompanied by a simultaneously occurring Signal Fail/Signal Degrade (set/clear) event on the Working line card.

Workaround: There is no workaround to prevent the symptom from occurring. However, when both interfaces are in the Active state, a manual or forced APS switch may restore sanity to the APS states.

- CSCeh17756

Symptoms: The PIM assert mechanism may not function properly, causing PE routers to remove VRF subinterfaces from output interface lists, and, in turn, causing multicast traffic to be dropped.

Conditions: This symptom is observed when redundant PE routers and CE routers are located on one LAN segment and when the CE routers select different PE routers as their next hop.

Workaround: Change the configuration in such a way that all CE routers on one LAN segment select the same PE router as their next hop.

- CSCeh18195

Symptoms: Packets that flow to VPNv4 destinations may be dropped for up to one second when the next-hop router clears its IS-IS overload bit after having been rebooted.

Conditions: This symptom is observed in a MPLS-TE network with one-hop TE tunnels.

Workaround: There is no workaround.

- CSCeh20156

Symptoms: With automatic protection switching (APS) configuration on CHOC12 Internet Services Engine (ISE) cards, flapping the working link within 2-3 sec time interval will result in some of the T1 links staying down.

Conditions: This symptom has been observed with APS configuration on a CHOC12 ISE card.

Workaround: A reload of the card is needed to clear the problem.
- CSCeh20201

Symptoms: Traffic entering a 1-port channelized OC-12/STM-4 (DS1/E1) ISE line card is dropped.

Conditions: This symptom is observed on a Cisco 12000 series when an MLP interface is moved from the 1-port channelized OC-12/STM-4 (DS1/E1) ISE line card to another line card.

Workaround: There is no workaround.
- CSCeh20219

Symptoms: The policer does not function for nxDs0 interfaces.

Conditions: This symptom is observed on a Cisco 12000 series that is configured with a 1-port channelized OC-12c/STM-4 (DS1/E1) ISE line card.

Workaround: There is no workaround.
- CSCeh23047

Symptoms: After a manual SSO switchover, traffic in the tag switching-to-IP switching direction between an egress 1-port 10-Gigabit Ethernet Engine 4+ line card and an ingress 4-port Gigabit Ethernet ISE line card does not recover.

Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of Cisco IOS Release 12.0(31)S. However, the symptom is platform-independent and may also occur on other platforms that function in a similar configuration and that run other releases.

Workaround: Reload microcode onto the 4-port Gigabit Ethernet ISE line card.
- CSCeh27734

Symptoms: For recursive routes with implicit null as the local label, the FIB may point to the rewrite of the parent prefix. However, this situation may not affect any functionality.

Conditions: This symptom is observed on a router that is configured for MPLS forwarding.

Workaround: Change the affected prefix to be non-recursive.
- CSCeh31764

Symptoms: A standby PRE that runs Cisco IOS Release 12.2S may crash when the primary PRE runs Cisco IOS Release 12.0S.

Conditions: This symptom is observed on a Cisco 10000 series when the primary RP is the PRE1 and runs Cisco IOS Release 12.0S and when the standby RP is PRE2 and runs Cisco IOS Release 12.2S in preparation for an upgrade switchover procedure. Due to a major version mismatch, the RPR mode is invoked automatically.

Workaround: There is no workaround.
- CSCeh33574

Symptoms: An Engine 4 plus or Engine 5 line card does not come up.

Conditions: This symptom is observed on a Cisco 12000 series that runs a Cisco IOS interim release for Release 12.0(31)S when IPC timeout errors occur.

Workaround: There is no workaround.

- CSCeh34989

Symptoms: One of the following two symptoms may occur on a POS ISE egress line card:

- The interface may become stuck during transmission. The line protocol will continuously flap because the interface continues to receive keepalives but is not able to send any keepalives.
- The line card generates the following harmless error message:

```
%EE48-4-GULF_TX_SRAM_ERROR: ASIC GULF: TX bad packet header detected. Details=0x4000
```

Conditions: These symptoms are observed on a Cisco 12000 series when an invalid packet is forwarded to an egress interface on an ISE line card.

Workaround: If the transmission on the interface is stuck, reload the line card by entering the **hw-module slot x reload** command.

- CSCeh36824

Symptoms: When the HA mode is RPR+ and a standby PRE comes up after a crash, the HA mode may change from RPR+ to SSO and the standby PRE displays error messages that indicate that the running configuration of the active PRE is “mode rpr-plus” but the running configuration of the standby PRE is “mode sso.”

When the HA mode is SSO and a standby PRE comes up after a crash, the standby PRE may become stuck in its initialization and does not enter the “STANDBY_HOT” state.

Conditions: These symptoms are observed on a Cisco 10000 series when the standby PRE crashes but does not report a switchover (that is, a “standby down” event occurs but not a switchover event), causing the standby PRE to come up in an inconsistent state. When the standby PRE crashes, the active PRE shows an error message that includes the text “PEER_CRASH_INTERRUPT.”

Workaround: Reset the standby PRE by entering the **hw-module standby-cpu reset** command to enable it to reload and come back up properly.

- CSCeh37351

Symptoms: In a tag switching-to-IP switching scenario with an ISE ingress line card and an Engine 4 plus (E4+) egress line card, the following bad packets may be forwarded to the E4+ line card:

- tag2ip, with bad ip hdr cksum
- tag2ip, with ip->tl > L2
- tag2ip, with ip->tl < 20
- tag2ip, with ip options packets
- tag2ip, with ip options packets with bad ip hdr cksum
- tag2ip, with ip options packets with ip->tl > L2
- tag2ip, with ip options packets with ip->tl < 20

These bad packets cause packet corruption and an “TX192-3-PAM_PIM” error message on the E4+ line card and may even cause the E4+ line card to reset.

Conditions: This symptom is observed on a Cisco 12000 series.

Workaround: There is no workaround.

Further Problem Description: The fix for this caveat enables the ISE line card to drop the above-mentioned bad packets.

- CSCeh39904

Symptoms: After removing a large number of Frame Relay subinterfaces, the following log is displayed:

SYS-3-CPUHOG: Task ran for 38160 msec (3/2), process = MDFS LC Process, PC = 41129150

Conditions: This symptom is observed on a Cisco 12000 series that is configured for Multicast VPN.

Workaround: There is no workaround.

- CSCeh40556

Symptoms: Links flap on a 1-port channelized OC-12/STM-4 (DS1/E1) ISE line card after an RP switchover has occurred.

Conditions: This symptom is observed on a Cisco 12000 series that has two PRPs and that runs Cisco IOS Release 12.0(31)S.

Workaround: There is no workaround.

- CSCeh40882

Symptoms: On a Cisco 12000 series router with a 1xChOC12/DS1 ISE line card configured with multilink MFR protocol and a MQC policy, after a reload the QoS does not get applied to the bundle. The QoS goes to the suspend mode.

Conditions: The bundle loses its QoS policy when the router is reloaded. This problem is observed when running Cisco IOS Releases 12.0(28)S1, 12.0(30)S, and an interim release for Release 12.0(31)S.

Workaround: Remove the service-policy from the bundle and re-apply it.

- CSCeh46072

Symptoms: When the following sequence is performed on a GSR, multiple subinterfaces will end up with the same ifnumber, thus resulting in incorrect CEF entries:

1. add serial subinterface (channelized). 2. delete the interface created. 3. add ATM subinterface. 4. add back the serial subinterface.

Conditions: This symptom occurs only if the above (or similar) sequence of adding and deleting subinterface is done.

Workaround: Do not delete and re-add the same subinterface. Instead, enter the **shut** command and then the **no shut** command. The same effect is achieved without running into the above symptom.

- CSCeh49881

Symptoms: In a tag switching-to-IP switching scenario with an ISE ingress line card and an Engine 4 plus (E4+) egress line card, the following bad packets may be forwarded to the E4+ line card:

- tag2ip, with bad ip hdr cksum
- tag2ip, with ip->tl > L2
- tag2ip, with ip->tl < 20
- tag2ip, with ip options packets
- tag2ip, with ip options packets with bad ip hdr cksum
- tag2ip, with ip options packets with ip->tl > L2
- tag2ip, with ip options packets with ip->tl < 20

These bad packets cause packet corruption and an “TX192-3-PAM_PIM” error message on the E4+ line card and may even cause the E4+ line card to reset.

Conditions: This symptom is observed on a Cisco 12000 series.

Workaround: There is no workaround.

Further Problem Description: The fix for this caveat enables the ISE line card to drop the above-mentioned bad packets.

- CSCeh51720

Symptoms: When the router is configured with a new area, the links that are configured for TE are not flooded in the new area.

Conditions: This symptom is observed when you configure an area by entering the **mpls traffic-eng area number** command as part of the router OSPF configuration.

Workaround: There is no workaround.

- CSCeh53373

Symptoms: A TE tunnel does not come up.

Conditions: This symptom is observed in an MPLS TE interarea configuration.

Workaround: There is no workaround.

- CSCeh55841

Symptoms: When you remove one CSC or one SFC, all traffic stops because there is insufficient fabric bandwidth. However, when you re-insert the CSC or SFC, all interfaces remain down.

Conditions: This symptom is observed on a Cisco 12000 series.

Workaround: Reload the router.

- CSCeh56377

Symptoms: VRF RP mapping continues to toggle between the RPs of two CE routers.

Conditions: This symptom is observed when a Cisco 12000 series that functions as a PE router is located between the two CE routers.

Workaround: Reset the PIM neighbor for the CE router that has the lower IP address of the two CE routers.

- CSCeh58485

Symptoms: It may take up to 180 seconds for a Parallel eXpress Forwarding (PXF) engine to reload after a toaster crash has occurred.

Conditions: This symptom is observed on a Cisco 10000 series that has a configuration with 200 VPN routing/forwarding instances and occurs only when the PXF engines restarts because of some kind of fault. The symptom does not occur when you enter the **microcode reload pxf** command.

Workaround: There is no workaround.

- CSCeh59452

Symptoms: An RP switchover may cause a 6-port channelized T3 Engine 0 line card to fail.

Conditions: This symptom is observed on a Cisco 12000 series that runs a Cisco IOS interim release for Release 12.0(31)S, that has two PRPs, and that functions in RPR+ redundancy mode.

Workaround: There is no workaround.

- CSCeh60185

Symptoms: An Engine 4 plus (E4+) line card that functions in an IP-to-tag switching scenario may generate “TX192-3-PAM_MODULE” and “%TX192-3-PAM_PIM” error messages and tracebacks or may crash.

Conditions: This symptom is observed on a Cisco 12000 series when the ingress interface is an Engine 2 line card that has an input ACL and when an external LDP flap occurs that affects the Engine 4+ line card.

Workaround: There is no workaround.

- CSCeh64632

Symptoms: After a route processor or line card has reloaded, the queue limit that is set for the class default is not properly programmed.

Conditions: This symptom is observed on a Cisco 12000 series 1-port channelized OC-12/STM-4 (DS1/E1) ISE line card that has an egress policy applied to a serial interface.

Workaround: There is no workaround.

- CSCeh65748

Symptoms: A Engine 3 ISE line card may not properly handle incoming bad IP packets but may generate a traceback and a transient error message:

```
%GSR-3-INTPROC: Process Traceback= 400E10B4 400FBA2C
-Traceback= 4047917C 405E5274 400F4B58
%EE48-3-BM_ERRS: FrFab BM SOP error 40000
%EE48-3-BM_ERR_DECODE: FrFab SOP macsopi_bhadr_pkt_len_zero_err
```

```
%GSR-3-INTPROC: Process Traceback= 400E1090 400FBA2C
-Traceback= 4047917C 405E5274 400F4B58
%LC-4-ERRRECOVER: Corrected a transient error on line card.
```

The line card may also crash.

Conditions: These symptoms are observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(26)S1 or Release 12.0(26)S5a.

Workaround: There is no workaround.

- CSCeh73978

Symptoms: When configuring service policies on any interface, the console erroneously displays a message indicating that Rate Limit and Policing can only be configured together on 4 port ISE Ethernet cards. More importantly, it prevents the service policy from being applied to the interface.

Conditions: This symptom has been observed on startup or anytime the configuration is entered.

Workaround: There is no workaround.

- CSCeh84320

Symptoms: The subinterface on the modular GE/FE card stops forwarding.

Conditions: This symptom occurs whenever the operator enters sub-interface mode with an xconnect statement on the EPA-GE/FE-BBRD fixed port on the modular GE/FE card.

Workaround: While in the sub-interface mode, the operator can enter a **shutdown** command followed by a **no shutdown** command which allows the subinterface to resume forwarding.

Each time the operator enters the sub-interface on the fixed port, the workaround will need to be applied.

- CSCeh84740

Symptoms: RPR+ switchover may cause the line card to pause indefinitely.

Conditions: This symptom has been observed when a high load of traffic is going through QoS configured interfaces on line cards.

Workaround: There is no workaround.

- CSCeh97080

Symptoms: When Multiprotocol Label Switching (MPLS) is enabled on a router, one or more LDP sessions may be disrupted during periods of extremely high CPU use.

Conditions: This symptom is observed when the CPU use of the router temporarily increases to more than 90 percent for several tens of seconds and when one or more high-priority processes are frequently active but do not necessarily use many CPU cycles.

For example, high CPU use may occur when a peer router is reloaded or when an interface with several hundreds of numbered IP subinterfaces comes up, which causes many processing changes on the router because of the “Tagcon Addr” process.

On a Cisco 12000 series, high CPU use may occur because of the “Fabric ping” high-priority process, which is frequently active.

Other high-priority processes may also cause the symptom to occur.

Workaround: To increase the length of the hello adjacency holdtimes, enter the **mpls ldp discovery hello holdtime** command on the affected router. You may need to enter this command on all platforms in the network in order to provide full protection.

- CSCeh97760

Symptoms: In the outputs of the **show ip psa-cef** and **show ip cef** commands for an Engine 2 ingress line card, the “Local OutputQ (Unicast)” information may point to another and incorrect slot than the slot that the global CEF table points to.

When this symptom occurs, packets that are destined for these specific IP address are dropped.

Conditions: This symptom is observed on a Cisco 12000 series when an Engine 2 line card is used as an ingress line card for traffic that is directed to a default route.

Workaround: Enter the **clear ip route 0.0.0.0** or **clear ip route *** command.

- CSCeh97829

Symptoms: An RP may crash continuously when you reload all the line cards in a dual-RP router that has the redundancy mode is set to SSO.

Conditions: This symptom is observed on a Cisco 12000 series that is configured with two GRPs or two PRPs that are configured for SSO and occurs only when a 1-port channelized OC-48 ISE line card, a 4-port channelized OC-12 ISE line card, or 16-port channelized OC-3 ISE line card is present in the router.

Workaround: Set the redundancy mode to RPR or RPR+.

- CSCei00027

Symptoms: On a channelized OC48 ISE line card with APS configured, the Signal Failure condition is retained after a line card reloads or after administratively entering the **shutdown** command and the **no shutdown** command.

Conditions: This symptom is specific to the Cisco 12000 router platform and affects only channelized OC48 ISE line card with APS configuration.

Workaround: There is no workaround.

- CSCin88273

Symptoms: After an RPR+ or SSO switchover occurs, an MLP sequence number mismatch may occur, a ping between back-to-back interfaces may not go through, and the routing protocol through this link may go down.

Conditions: This symptom is observed on a Cisco 7500 series that is configured for dMLP and RPR+ or SSO.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the multilink interface of the Cisco 7500 series.

- CSCin88356

Symptoms: The output of the **show interfaces serial number** command does not show the total output packet drops.

Conditions: This symptom is observed when you apply a service policy on an interface that is configured for CEF.

Workaround: Enter the **show policy map interface interface-name** command to see the total output packet drops.

- CSCsa41907

Symptoms: When a channel group is removed from and added to a controller and when a PRE switchover occurs, the line protocol on another channel goes down after a while and input packets are not counted.

Conditions: This symptom is observed on a Cisco 10000 series that is configured with 6-port channelized T3 line card.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface.

Alternate Workaround: Ensure that the you enter the **hw-module standby-cpu reset** command before a PRE switchover occurs.

- CSCsa43329

Symptoms: A Cisco 12000 series may crash because of a bus error when you configure a loopback on one of the E3 interfaces on a 6-port E3 (6E3-SMB) or 12-port E3 (12E3-SMB) line card.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S.

Workaround: Do not configure a loopback on one of the E3 interfaces.

- CSCsa49906

Symptoms: When loopback is removed from a T1 interface of a CT3 controller, the following warning message is encountered with a removal of the loopback being denied:

```

GSR(config)#cont t3 7/5 GSR(config-controller)#no T1 5 loopback
%Inband loopback is already running on T1 12. Only one code can be running per T3 at
a time GSR(config-controller)#

```

Conditions: The symptom is observed after upgrading to Cisco IOS Release 12.0 (27)S2 on a Cisco 12000 Series Gigabit Switch Router with a 6CT3 linecard.

Workaround: There is no workaround.

- CSCsa53685

Symptoms: Incorrect VC12 defect information may be generated on a Cisco 7500 series that is configured with a PA-MC-STM-1.

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(28)S1.

Workaround: There is no workaround.

- CSCsa54891

Symptoms: Under normal operation, an Engine 6 line card may reset with the following error messages and tracebacks:

```
%TX192-3-CPUIF: Error=0x10
```

```
rd 0x73 base 0x73 hdr 0x75 last 0x75 wr 0x75
insert 0x0 back 0x0 len 0x2474 cnt 0x0
```

```
-Traceback= 40D89758 405A9008 405EC67C 406D5E7C 406D64F8 400FC020
```

```
%TX192-3-CPUIF_ERR: FIFO RAM3 Parity Error.
```

```
-Traceback= 40D89808 405A9008 405EC67C 406D5E7C 406D64F8 400FC020
```

```
%GSR-3-INTPROC: Process Traceback= 400FFD20 400FCAA0 40010F6C
```

```
-Traceback= 404EFBCC 406D6760 400FC020
```

```
%FABRIC-3-ERR_HANDLE: Due to FIA HALT error, reconfigure FIA on slot 9
```

Conditions: This symptom is observed on a Cisco 12000 series when false RAM parity errors occur.

Workaround: There is no workaround.

Further Problem Description: The fix for this caveat determines whether the RAM parity errors are real or false.

- CSCsa55048

Symptoms: The content of the CEF table may be incorrect, causing less than optimal traffic conditions.

Conditions: This symptom is observed when a static route is configured in one VRF and exported with an export map into another VRF and when this static route is added on two separate PE routers.

Workaround: Do not configure the static router on both PE routers. If this is not an option, there is no workaround.

- CSCsa57562

Symptoms: IPC messages may be generated on a 1-port channelized OC-12 (DS3) line card and the line card may be disabled and reload.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S or Release 12.0(28)SW1 when OC-3 subinterfaces are configured on the 1-port channelized OC-12 (DS3) line card, when these OC-3 subinterfaces are configured for Frame Relay, when the **rate-limit** command is enabled, and when L2TPv3 traffic is being processed.

Workaround: There is no workaround because the **rate-limit** command is not supported in a configuration in which L2TPv3 traffic is being processed.

- CSCsa59109

Symptoms: At random, subinterfaces lose the ability to ping a directly-connected peer.

Conditions: This symptom is observed on a Cisco 12000 series that is configured with two 3-port Gigabit Ethernet line cards.

Note that although regular and extended pings do not work, pings that use the record option do work.

Workaround: Reload microcode onto the affected line cards.

- CSCsa59829

Symptoms: With traffic passing over a network only occasionally, a 4-port OC12 ATM ISE line card generates a “%PM622-3-CPK24_INTR: Egr SAR timeout” error message and resets.

Conditions: This symptom is observed on a Cisco 12000 series.

Workaround: Reload the line card.

Further Problem Description: The symptom occurs when the “CPK24 FPGA” detects that the SAR does not respond in the “Utopia interface.” The SAR then crashes because of a bad canonical header in the egress direction.

- CSCsa60026

Symptoms: Cells loss occurs on a single ATM link of PA-A3-8T1IMA or PA-A3-8E1IMA port adapter.

Condition: This symptom is observed on a Cisco 7500 and 7200 series when one of the T1 or E1 member interfaces of an IMA group that is configured on a PA-A3-8T1IMA or PA-A3-8E1IMA port adapter is disconnected or when you enter the **shutdown** command on one of these T1 or E1 member interfaces. The symptom is not platform-specific and may also occur in other releases.

Workaround: There is no workaround.

- CSCsa65732

Symptoms: When you remove a policy map from a subinterface, the subinterface may become stuck, preventing traffic from passing through the subinterface.

Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.0(25)SX7 when a nested policy map is applied to the main or physical interface in addition to the one that is already applied to the subinterface. The symptom could also occur in Release 12.0S.

Workaround: Remove the policy map from the physical interface before you remove the policy map from the subinterface. When the subinterface configuration is updated, re-apply the policy map to the physical interface.

- CSCsa67488

Symptoms: A Cisco 10008 router with PRE1 may report a PXF crash.

Conditions: The symptom is observed when modifying an access-list that is already attached to a multilink interface.

Workaround: Modify an access-list only if it not attached to the interface. If the access-list cannot be removed from the interface, then create a new one and apply.

- CSCsa68240

Symptoms: Interfaces of an Engine 4 POS line card may not enter the up/up state.

Conditions: This symptom is observed on a Cisco 12000 series after you have changed the Cisco IOS software image.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected POS interfaces to enable them to enter the up/up state.

- CSCsa68301

Symptoms: Inter-MVPN traffic does not function on an Engine 4+ line card.

Conditions: This symptom is observed on a Cisco 12000 series and may occur with any Engine 4+ line card.

Workaround: There is no workaround.
- CSCsa68616

Symptoms: An IPC failure occurs and an OC-12 line card that is configured for Frame Relay over MPLS resets.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(27)S1.

Workaround: There is no workaround.

Further Problem Description: The IPC failure and the line card reset occur after a depletion of the elements in the FrFab 608 byte queue for the line card. Consecutive outputs of the **show controllers slot-number frfab queue** command show a consistent and rapid leak of these buffers.
- CSCsa70274

Symptoms: A Cisco router may crash during an LSP traceroute when a transit router responds with a downstream map TLV that contains a multipath length field that is set to 0, 1, 2, or 3.

Conditions: This symptom is observed during testing of the Cisco LSP ping draft version 3 in a network that uses a later version of the LSP ping draft.

The implementation of draft version 3 does not handle the multipath length field settings correctly. In draft version 3 and earlier drafts, there is an ambiguity on whether or not the multipath length field includes the four bytes comprising of the hash-key type, depth limit, and multipath length fields. As such, all implementations of the draft version 3 encode the length as four bytes and reply with a multipath length of four bytes.

When an LSP traceroute is invoked and a transit router replies with a downstream map TLV that contains a multipath length field that is set to a length shorter than four bytes, existing implementations handle this situation incorrectly and cause memory packet memory to become corrupted during the subsequent attempt to build an MPLS echo request packet. This situation eventually causes the router to crash.

Workaround: If LSP traceroute implementations exist on a transit router that cause the transit router to reply with a multipath length that is set to a value other than four, avoid using an LSP traceroute.

Note, however, that the implementations of Cisco LSP ping draft version 3 do not reply with multipath lengths that can cause this crash.
- CSCsa77105

Symptoms: An LSP ping (or traceroute packet) is incorrectly sent from an unlabeled interface, preventing the LSP ping to detect LSP breakages when a one-hop label switched path is pinged.

Conditions: This symptom is observed on a Cisco router that is configured for MPLS OAM.

Workaround: There is no workaround.
- CSCsa80661

Symptoms: The data path on a 3-port Gigabit Ethernet Engine 2 (3GE-GBIC-SC) line card may be reset because of a corrupted packet that is found in the Tx SOP SRAM. This situation causes packet loss and the routing protocol sessions to flap.

Conditions: This symptom is observed on a Cisco 12000 series that runs a Cisco IOS software release that includes the fix for caveat CSCef06121. A list of the affected releases can be found at <http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCef06121>. Cisco IOS software releases that are listed in the “First Fixed-in Version” field at this location are affected.

Workaround: There is no workaround. The symptom causes a disruption of service, but service is restored.

Further Problem Description: When the symptom occurs, the following messages are generated in the log:

```
%RP-3-FABRIC_UNI: Unicast send timed out (1)
CORRUPT PACKET DUMP:
000005C000000000 0200000000000000 0000000101000000 00062AD9B40A0003 A09D008208004500
0000000000000000 0000000000000000 0000000000000000 0000000000000000 0000000000000000
0000000000000000 0000000000000000

%RPGE-6-AUTONEG_STATE: Interface GigabitEthernet1/0: Link OK - autonegotiation
complete
%RPGE-6-AUTONEG_STATE: Interface GigabitEthernet1/2: Link OK - autonegotiation
complete
%RPGE-6-AUTONEG_STATE: Interface GigabitEthernet1/1: Link OK - autonegotiation
complete
%LCGE-3-SOP_BAD_PACKET: Found corrupt pkts in tx-sop-sram. Data path was reset.

%OSPF-5-ADJCHG: Process 1, Nbr 10.142.65.38 on GigabitEthernet1/0 from LOADING to
FULL, Loading Done
%OSPF-5-ADJCHG: Process 1, Nbr 10.142.65.44 on GigabitEthernet1/2 from LOADING to
FULL, Loading Done
```

- CSCsa86214

Symptoms: Locally-originated and transit packets that are greater than 1599 bytes in length are not exiting the router. BGP and other TCP based protocols that negotiate large MSS values may go down.

Conditions: This symptom may occur when any PRE/PRE1-based Cisco 10000 router is doing IP fragmentation.

Workaround: Use the **show hardware pxf cpu buffer** command or **show pxf cpu buffers** command to verify buffer depletion. Perform a microcode reload of the PXF.

- CSCsa87295

Symptoms: Traffic to a network core is dropped from a link-bundle interface of an Engine 3 line card.

Conditions: This symptom is observed when the network core is a Cisco 12000 series that runs Cisco IOS Release 12.0(26)S or a later release, that functions as a PE router, that is configured for MPLS VPN, and that has L3 loadbalancing enabled on an egress path through a link-bundle interface.

Workaround: There is no workaround.

Further Problem Description: The symptom occurs because there is incorrect FCR information in the Engine-3 hardware rewrites that point to the link-bundle interface.

- CSCsa88211

Symptoms: When you boot a Cisco 12000 series, some Layer 1 and CoS command are rejected with the following error messages:

```
Command "pos threshold sd-ber 9" not allowed on link-bundle member interface POS1/0
Command "tx-cos TEST" not allowed on link-bundle member interface POS1/0
```

Conditions: This symptom is observed on a Cisco 12000 series when a POS interface of an Engine 0 or Engine 2 line card has the **tx-cos** command enabled and is a member of a port channel or POS channel.

Workaround: There is no workaround.

- CSCsa93814

Symptoms: Sending high-rate Multicast and Unicast bi-directional traffic can cause the PXF complex to pause indefinitely and recover.

Conditions: This symptom has been observed when sending IP Multicast, high- rate bi-directional Unicast and Multicast traffic between 4 GE ports across an SRP uplink.

Workaround: There is no workaround.

- CSCsa96275

Symptoms: When you send traffic with the full bandwidth of an IMA bundle, cell loss occurs. For example, cell loss occurs when you send traffic with more than 5 Mbps on an 8-link T1 IMA group or with 6.4 Mbps on an 8-link E1 IMA group.

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(30)S and that is configured for ATM L2TPV3, cell-packing, and multiple VP configurations. There is no cell loss with a single PVC without an L2TPv3 configuration.

Workaround: There is no workaround.

- CSCsa96941

Symptoms: When sending VBR ATM traffic through a 4-port ISE ATM OC3 to an L2TPv3 (over IP) tunnel and out another 4-port ISE ATM OC3 on another Cisco 12000 router, the ATM generator/analyzers are sending VBR traffic at lower rates than what is configured on the routers and cell loss is displayed on the traffic generator.

Conditions: This symptom has been observed when a Cisco 12000 router was connected back-to-back via POS OC192, ATM OC3 engine 3 configured with L2TPv3, or an ATM generator was connected to both Cisco 12000 ATM interfaces.

Workaround: There is no workaround.

- CSCsa97159

Symptoms: When you boot a Cisco 12000 series, CDP command is rejected with the following error messages:

```
Command " no cdp enable" not allowed on link-bundle member interface POS1/0
```

Conditions: This symptom is observed on a Cisco 12000 series that is configured with POS interfaces when interface POS1/0 is a member interface of a link bundle.

Problem does not happen with GE link bundle.

Workaround: There is no workaround.

- CSCsa99983

Symptoms: New AToM or L2TPv3 sessions may not come up.

Conditions: This symptom is observed on a Cisco router that is configured for Multilink Frame Relay (MFR) over L2TPv3/AToM when there are services with incomplete MFR over L2TPv3/AToM configurations and when the router has run for a long period of time.

Workaround: There is no workaround.

- CSCsb00493

Symptoms: No packets are switching through the core link on GSR if hw- acceleration is enabled on this line card.

Conditions: This symptom has been observed when a vrf interface is configured on the same line card as the core link and the vrf interface is shutdown.

Workaround: Disable hw-acceleration on the line card.

- CSCsb02964

Symptoms: The router pauses indefinitely when an access-list (ACL) that is too large and complex to fit in memory is applied to an MQC policy-map. When the class-map (with the offending ACL) is applied to a policy-map, the router pauses indefinitely with a MALLOCFAIL error while compiling the ACL.

Conditions: This symptom was observed when using a 2000 line complex ACL. Instead of reporting an out-of-memory situation, the router pauses indefinitely.

Workaround: There is no workaround since the ACL being applied is too large for the memory to support.

- CSCsb04721

Symptoms: When the Any Transport over MPLS (AToM) feature is enabled on a router, AToM virtual circuits to a peer may not be re-established after an interface flap or after being reconfigured, because the required targeted Label Distribution Protocol (LDP) session is not re-established.

Conditions: This symptom is observed when LDP is not configured on any interfaces via the **mpls ip** interface configuration command, which is typically the case when MPLS Traffic Engineering (TE) tunnels are used to transport AToM traffic between endpoints and when the **mpls ip** interface configuration command is not enabled on any TE tunnels.

The symptom occurs in Cisco IOS software releases that include the fix for caveat CSCec69982 when any form of one of the following commands is configured on the router and appears in the running configuration:

```
- mpls ldp explicit-null
- mpls ldp advertise-labels
- mpls ldp session protection
- mpls ldp password fallback
- mpls ldp password option
- mpls ldp password required
```

A list of the affected releases can be found at

<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCec69982>.

Workaround: Enter the **mpls ip** command on a TE tunnel interface or temporarily on a physical interface to force LDP to be re-established.

- CSCsb06383

Symptoms: When sending high rate Multicast and Unicast bi-directional traffic back to back between 4 Gigabit Ethernet ports and across the SRP uplink interface, the PXF complex occasionally stops running. The PXF complex restarts and functionality is restored automatically.

Conditions: This symptom has been observed with high rate Multicast and Unicast traffic.

Workaround: Recovery is automatic.

- CSCsb09190

Symptoms: An router configured as a Multiprotocol Label Switching (MPLS) VPN provider edge (PE) router misses an entry in its label forwarding table

Conditions: If the **show tag-switching forwarding-table** EXEC command is entered for the missing entry, no label is shown. And the **show ip cef detail** EXEC command is entered for the prefix, no label is shown.

This symptom is found on Cisco IOS Release 12.2(28).

Workaround There is no workaround. However, if you enter the **clear ip route** command for the affected prefix, the prefix is reinstalled in the label forwarding table.

Wide-Area Networking

- CSCef71011

Symptoms: Pings fail when translational bridging and ATM DXI encapsulation are configured.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0S, Release 12.2S, or a release that is based on Release 12.2S.

Workaround: Do not configure ATM DXI encapsulation. Rather, configure HDLC, PPP, or Frame Relay encapsulation.

- CSCeh33185

Symptoms: A POS interface on a VIP4-80 that is configured for PPP goes down and remains down.

Conditions: This symptom is observed on a Cisco 7513 that runs Cisco IOS Release 12.0S only when PPP receives an LCP PROTOCOL REJECT message for PAP or CHAP. The symptom may also occur in other releases.

Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the affected POS interface.

- CSCeh49910

Symptoms: With automatic protection switching (APS) configuration on CHOC12 Internet Services Engine (ISE) cards, flapping the working link within a 2- to 3-second time interval may result in some of the T1 links staying down.

Conditions: This symptom has been observed with APS configuration on a CHOC12 ISE card.

Workaround: Enter a **shutdown** command and then a **no shutdown** command to clear the problem.

Resolved Caveats—Cisco IOS Release 12.0(30)S2

Cisco IOS Release 12.0(30)S2 is a rebuild of Cisco IOS Release 12.0(30)S. The caveats listed in this section are resolved in Cisco IOS Release 12.0(30)S2 but may be open in previous Cisco IOS releases. This section describes only severity 1, severity 2, and select severity 3 caveats.

Miscellaneous

- CSCeh42465

Symptoms: An Engine 3 line card sends unlabeled traffic after it has been toggled from explicit routing to default routing. The symptom is related to the handling of a default-route on an Engine 3 ingress line card that functions in an IP-to-MPLS path.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(30)S1 or any other image that includes the fix for caveat CSCsa64782, which is a preliminary requisite for default-route handling on an Engine 3 line card. The symptom occurs in the following scenario:

1. You configure BGP to advertise the target address, so the target address is directly known in the routing table.
2. You remove the advertisement from BGP and return to default routing, with the same source for the next hop as the platform that was the BGP next hop.
3. You enter the **clear ip route network** command, with the address of the BGP next hop for the *network* argument.

After the transition from non-default routing to default routing, entering the **clear ip route network** command, with the address of the next hop for the *network* argument, causes an inconsistency, and traffic is forwarded as unlabeled.

Workaround: To restore proper operation, enter the **clear ip route 0.0.0.0** command.

Resolved Caveats—Cisco IOS Release 12.0(30)S1

Cisco IOS Release 12.0(30)S1 is a rebuild of Cisco IOS Release 12.0(30)S. The caveats listed in this section are resolved in Cisco IOS Release 12.0(30)S1 but may be open in previous Cisco IOS releases. This section describes only severity 1, severity 2, and select severity 3 caveats.

Basic System Services

- CSCed64664

Symptoms: A “%SYS-2-LINKED: Bad enqueue” error message may be seen in the syslog of an LNS right after traffic is sent through a PPP multilink bundle that is established via an L2TP session on the LNS. This message is also seen when multilink PPP fragments are switched or when multicast packets are replicated.

Certain packet buffers (particle clones) are eventually depleted, and multilink fragmentation stops working when all particle clones are exhausted. You can monitor the availability of particle clones by entering the **show buffers | begin Particle Clones: EXEC** command; the command does not produce any output if no more particle clones are available.

Conditions: This symptom is observed with all features that use particles. The symptom is not specific to VPDN, GRE, or other features that use particles.

Workaround: There is no workaround.

Further Problem Description: Different symptoms may occur with different features.

- CSCee83917

Symptoms: The RP of a Cisco router may crash when entering the **write memory** legacy command.

Conditions: This symptom is observed on a Cisco router that has the **snmp mib community-map** command enabled with a very long community string and an engineID. The symptom may also occur when the long community string is removed from the configuration. The symptom does not occur when entering the **copy running-config startup-config** EXEC command.

Workaround: A community string that is shorter than 40 characters will not cause the symptom to occur.

- CSCeg15044

Symptoms: Although there are free tty lines, you cannot make a Telnet connection and a “No Free TTYs error” message is generated.

Conditions: This symptom is observed when there are simultaneous Telnet requests.

Workaround: There is no workaround.

- CSCeg23428

Symptoms: After you perform an OIR of a VIP, reload microcode onto a VIP, or after a VIP crashes, an MLP or MFR interface that is shut down comes up unexpectedly.

Conditions: This symptom is observed on a Cisco 7500 series only with virtual interfaces and only the first time that you perform an OIR or reload microcode or that the VIP crashes after the router has booted up. The symptom does not occur when you perform subsequent OIRs or reload microcode again or when the VIP crashes again.

Workaround: There is no workaround.

- CSCin79312

Symptoms: An outage may occur when you attempt to connect via the console port to a Cisco ONS 15540, and routine messages are generated that relate to the loss of light on wave ports that are turned on. Interface alarm flaps may cause a hardware watchdog timeout, and the platform may fail to switch over to the standby CPU.

Conditions: These symptoms are observed on a Cisco ONS 15540 during normal operation when optical interfaces are not used not shut down.

Workaround: There is no workaround. Customer should shut any unused interfaces.

Interfaces and Bridging

- CSCeb60620

Symptoms: A Cisco Route Switch Processor (RSP) that is configured as a bridge may not pass bridged traffic, regardless of the protocols that are configured on Ethernet interfaces. This situation can lead to a loss of connectivity.

Conditions: This symptom is observed on a Cisco RSP that is running a Cisco IOS rsp-jsv-mz image.

Workaround: There is no workaround.

- CSCef79968

Symptoms: When an snmpget is executed for an interface index below .1.3.6.1.2.1.31.1.1.1.6, the router responds with the following information:

```
ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifHCInOctets.12 : VARBIND EXCEPTION: No Such Instance
```

However, an snmpwalk executes successfully for an interface index below .1.3.6.1.2.1.31.1.1.1.6.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(26)S3 when an snmpget is executed for 4GE-SFP-LC subinterfaces or for a 4GE-SFP-LC interface when there is another interface index for the same interface. The symptom may be platform-independent.

Workaround: Reload the router.

- CSCeg03185

Symptoms: A few permanent virtual circuits (PVCs) go into a stuck state causing OutPktDrops on a Cisco 7200 router.

Conditions: This symptom occurs on a Cisco 7200 router running Cisco IOS Release 12.2(26) with a PA-A3-T3 ATM interface. The symptom may also occur in other releases.

Workaround: Remove and re-apply the PVC statement.

IP Routing Protocols

- CSCdr31946

Symptoms: A Cisco router that runs Enhanced Interior Gateway Routing Protocol (EIGRP) with the stub feature enabled may have a route that is active and not waiting for replies.

Conditions: This symptom is observed only in networks where all of the EIGRP neighbors are declared as stub.

Workaround: Remove the EIGRP stub feature or clear the IP EIGRP neighbors.

- CSCed93804

Symptoms: EIGRP may incorrectly remove a connected route from a topology.

Conditions: This symptom is observed when you change the router network commands and there are overlapping networks. For example, if the following is configured:

```
int loopback1 ip addr 10.1.2.2 255.255.255.0
router eigrp 1 net 10.0.0.0 0.3.255.255
and you change the network command to:
router(config-router)# net 10.0.0.0 router(config-router)# no net 10.0.0.0
0.3.255.255
```

the connected route will be removed when it should be retained.

Workaround: Remove the old network command first before adding the new one, for example:

```
router(config-router)# no net 10.0.0.0 0.3.255.255
router(config-router)# net 10.0.0.0
```

- CSCef45830

Symptoms: A stale BGP route does not time out, which can be observed in the output of the **show ip route vrf** command.

Conditions: This symptom is observed in a BGP multipath configuration.

Workaround: Enter the **clear ip route vrf vrf-name** command.

- CSCef57803

Symptoms: In a VPNv4 network in which a multi-homed CE router advertises multiple paths for a prefix, a PE router may fail to withdraw the prefix previously advertised to another PE router when its best path changes from a non-imported path to an imported path because of a change in the import route map of the VRF.

Conditions: This symptom is observed in a topology in which a CE router connects to a PE router via two different VRFs.

Workaround: Remove the imported path either by unconfiguring the import route map of the VRF or by changing the import route target, withdraw the non-imported prefix from the CE router, and restore the import route map or import route target.

- CSCef60659

A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP “hard” error messages.
2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks.
3. Attacks that use ICMP “source quench” messages.

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml>.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected.

- CSCef65500

Symptoms: A Cisco router that is configured for OSPF may generate recurring SYS-3-CPUHOG messages and tracebacks that are caused by the OSPF process:

```
%OSPF-5-ADJCHG: Process 100, Nbr 10.52.0.186 on ATM1/0.381 from LOADING to
FULL, Loading Done
%SYS-3-CPUHOG: Task ran for 4568 msec (243/31), process = OSPF Router, PC =
60B9DFA8.
-Traceback= 60B9DFB0 60B7E6E0 60B7EE58
%OSPF-5-ADJCHG: Process 100, Nbr 10.53.0.66 on ATM1/0.115 from FULL to DOWN,
Neighbor Down: Dead timer expired
%OSPF-5-ADJCHG: Process 100, Nbr 10.53.0.66 on ATM1/0.115 from LOADING to
FULL, Loading Done
%SYS-3-CPUHOG: Task ran for 4988 msec (569/120), process =
OSPF Router, PC = 60B9DFA8.
-Traceback= 60B9DFB0 60B7E6E0 60B7EE58
```

At another date, the following error messages and tracebacks are generated:

```
%SYS-3-CPUHOG: Task ran for 2224 msec (368/9), process = OSPF Router, PC =
60BA80BC.
-Traceback= 60BA80C4 60B8876C 60B88EE4
%OSPF-5-ADJCHG: Process 100, Nbr 10.61.0.26 on ATM2/0.179 from FULL to DOWN,
Neighbor Down: Dead timer expired
%OSPF-5-ADJCHG: Process 100, Nbr 10.61.0.26 on ATM2/0.179 from INIT to DOWN,
Neighbor Down: Interface down or detached
```

```
%OSPF-5-ADJCHG: Process 100, Nbr 10.61.0.26 on ATM2/0.179 from LOADING to
FULL, Loading Done
%SYS-3-CPUHOG: Task ran for 2028 msec (647/283), process = OSPF Router, PC =
60BA80BC.
-Traceback= 60BA80C4 60B8876C 60B88EE4
%SYS-3-CPUHOG: Task ran for 2904 msec (552/153), process = OSPF Router, PC =
60BA80BC.
-Traceback= 60BA80C4 60B8876C 60B88EE4
```

Conditions: This symptom is observed on a Cisco 7200 series that is configured with an NPE-225 and that runs Cisco IOS Release 12.2(15)T5 or 12.2(15)T13. However, the symptom may be platform-independent and could also occur in other releases.

Workaround: There is no workaround.

- CSCef91275

Symptoms: An MPLS TE tunnel stays stuck in the “Path Half Admitting” state, as is shown by the output of the **show mpls traffic-eng tunnel** command, thereby preventing the tunnel from coming up.

Conditions: This symptom may be observed when a particular third-party router that functions as the headend for the MPLS TE tunnel sends a Path message to a Cisco router that functions as the midpoint for the router MPLS TE tunnel and that does not have the **mpls traffic-eng tunnels** interface configuration command enabled on the outbound interface that would be used to forward the Path message.

Workaround: Enter the **mpls traffic-eng tunnels** interface configuration command on the outbound interface of the Cisco router. Then, enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on this interface, and save the configuration.

- CSCef92863

Symptoms: A Cisco 10000 PRE-1 may reload when a VRF that is configured with eight maximum paths is modified.

Conditions: This symptom is observed when a VRF on the Cisco 10000 series is configured for eight maximum EIBGP paths by entering the **maximum-paths eibgp 8** command and when the VRF is modified in such a way that there is a change in the number of paths that are available. The symptom may also occur on a Cisco 10720.

Workaround: A Cisco 10000 series can support only six maximum paths. Therefore, configure the number of maximum paths by entering the **maximum-paths eibgp 6** command.

- CSCef93215

Symptoms: A router that is configured for OSPF may reload unexpectedly and reference the “ospf_build_one_paced_update” process.

Conditions: This is observed on a Cisco router that has a mixture of LSAs (of type 5 and 11) that travel throughout an autonomous system and LSAs (of any type other than type 5 and 11) that travel within a particular OSPF area. The symptom may occur at any time without any specific changes or configuration and is not specifically related to any type of LSA.

Workaround: There is no workaround.

Further Problem Description: The symptom is very unlikely to occur. The symptom does not occur on a router that has exclusively stub areas and NSSA areas. The symptom may occur when a router does not have exclusively stub areas and NSSA areas.

- CSCef97738

Symptoms: BGP may pass an incorrect loopback address to a multicast distribution tree (MDT) component for use as the source of an MDT tunnel.

Conditions: This symptom is observed when you reload a Cisco router that runs Cisco IOS Release 12.0(28)S1 and when there is more than one source address that is used in BGP, such as Lo0 for IPv4 and Lo10 for VPN. If the IPv4 peer is the last entry in the configuration, the MDT tunnel interface uses lo0 as the source address instead of lo10. The symptom may also occur in other releases.

Workaround: Remove and add the MDT statement in the VRF.

- CSCeg19442

Symptoms: A router that is configured with the OSPF routing protocol may reload.

Conditions: This symptom is observed when the OSPF process is simultaneously deconfigured via one session and configured via another session.

Workaround: There is no workaround. Cisco strongly discourages you to configure a router via two different but simultaneous sessions.

- CSCeg30291

Symptoms: BGP fails to send an update or withdraw message to some peers when these peers have failed to converge properly after an earlier attempt.

Conditions: This symptom is observed on a Cisco router when you enter the **clear ip bgp neighbor-address soft out** command while BGP is in the middle of converging. The symptom does not occur when network traffic load is low and BGP has converged.

Workaround: To clear the error condition, enter the **clear ip bgp neighbor-address soft out** command again. Alternately, enter the **clear ip bgp neighbor-address** command (that is, without the **soft out** keyword).

- CSCeg49796

Symptoms: Commands on a router may be unexpectedly removed from the running configuration.

Conditions: This symptom is observed on a router that is assigned as a neighbor to a BGP peer group. For example, when the **shutdown** command was previously configured on the router, the command is removed from the running configuration after the router is assigned as a neighbor to a BGP peer group.

Workaround: Re-enter the commands on the router.

- CSCin74330

Symptoms: The LDP Hello process may not be reinitiated after a TDP ID is received, preventing LDP neighbors from being discovered.

Conditions: This symptom is observed on a Cisco router that does not have an IP address configured when you first enter the **mpls ip** command and then assign the IP address.

Workaround: Assign the IP address to an interface of the router before you enable MPLS.

- CSCsa40588

Symptoms: Routes may still appear in the routing table even after the routes are removed from the BGP table.

Conditions: This symptom is observed on a Cisco platform that functions as a PE router when a CE router stops advertising a BGP route to the PE router. The BGP table reflects the route change but the routing table still indicates that the route is valid.

Workaround: There is no workaround.

- CSCuk54787

Symptoms: When a route map is configured, routes may not be filtered as you would expect them to be filtered.

Conditions: This symptom is observed on a Cisco router that is configured for BGP and that functions in an MPLS VPN environment.

Workaround: There is no workaround.

ISO CLNS

- CSCsa45381

Symptoms: CLNS fast-switching is disabled on a serial E3 interface that is configured for HDLC encapsulation.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(30)S but may also occur in other releases.

Workaround: There is no workaround.

Miscellaneous

- CSCdw00559

Symptoms: When you attempt to delete an entry from the ipNetToMediaTable table and if the associated ifIndex value is greater than the number of nonvirtual interfaces in the system, you cannot delete the entry successfully and receive a “WrongValue” error.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.1E but may also occur in other releases.

Workaround: There is no workaround.

- CSCeb84128

Symptoms: A Cisco 10000 series may stop responding.

Conditions: This symptom is observed when you attach a child policy map with four policing statements to a parent policy map with a bandwidth queue and when the parent policy map is already attached to 100 T1 interfaces.

Workaround: Attach the child policy map to the parent policy map before you attach the parent policy map to the interfaces.

- CSCec51408

Symptoms: After you reload a Cisco 7xxx series router, the **vbr-nrt output-pcr output-scr output-mbs** command or the **ubr output-pcr** command may be missing from the configuration of the IMA-group interface of a PA-A3-8T1IMA or PA-A3-8E1IMA port adapter.

Conditions: The symptom is observed when the **vbr-nrt output-pcr output-scr output-mbs** command or the **ubr output-pcr** command is configured on an IMA-group interface that also has minimum active links configured.

Workaround: There is no workaround.

- CSCed63900

Symptoms: Counters in the output of the **show policy-map interface** command are incorrect because locally generated traffic such as control plane messages are counted twice.

Conditions: This symptom is observed on a Cisco 10000 series that has interfaces on which outgoing QoS policy map is configured.

Workaround: There is no workaround.

- CSCed95499

Symptoms: A Cisco router may crash if a PA driver attempts to convert an uncached iomem address to a cached iomem address.

Conditions: This symptom is observed on a Cisco 7200 series that is configured with an NPE-G1.

Workaround: There is no workaround.

- CSCee16205

Symptoms: The committed information rate (CIR), normal burst, and maximum burst of the **police** (percent) command in a policy map are set incorrectly.

Conditions: This symptom is observed when the policy map is attached to an MLP interface that is configured for LFI and that is in the “DOWN” state.

Workaround: Attach the policy map when the MLP interface is in the “UP” state.

- CSCee66058

Symptoms: SNMP users that have MD5 configured may become lost after a switchover in an RPR+ environment.

Conditions: This symptom is observed on a Cisco 7500 series and Cisco 12000 series that run Cisco IOS Release 12.0(27)S1 in RPR+ mode.

Workaround: There is no workaround.

- CSCee66214

Symptoms: A VIP may crash with a bus error after you have configured a multilink interface.

Conditions: This symptom is observed after you have configured a multilink interface with serial interfaces on a PA-MC-8TE1+ and PA-MC-8E1/120 port adapter.

Workaround: Use the same type of port adapter for each multilink interface.

- CSCee67278

Symptoms: A VIP may crash with a bus error and generate the following error message:

```
%ALIGN-1-FATAL: Illegal access to a low address
```

This occurs after the following scheduler error in the “req_proc” process:

```
%SYS-2-INTSCHED: 'sleep for' at level 2 -Process= "req_proc", ipl= 2, pid= 27
```

Conditions: This symptom is observed on a Cisco 7500 series that runs a Cisco IOS image that contains the fix for CSCec07487 when a PA-MC-8TE1+ is installed in the VIP.

Workaround: There is no workaround.

- CSCef16379

Symptoms: An Engine 2 8-port ATM line card may not forward traffic from a VRF.

Conditions: This symptom is observed on a Cisco 12000 series when the prefix of the VRF is imported using an MPBGP tag.

Workaround: There is no workaround.

- CSCef18515

Symptoms: After you have entered the **clear cef line** command, when you enter the **show ip cef** command for the RP and for a line card, the output is inconsistent.

Conditions: This symptom is observed on a Cisco 12000 series that runs a Cisco IOS interim release for Release 12.0(30)S and that is configured for Fast ReRoute.

Workaround: There is no workaround.

- CSCef25917

Symptoms: A 4GE-SFP-LC line card may reload unexpectedly when it processes QoS traffic in a configuration with a VLAN on a VCG that is configured with an ingress CoS.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(26)S or a later release when the resolved ARPs are deleted, for example, when routers flap, when BGP peers do not respond, or when you enter the **clear arp** command. Note that the symptom may also occur on releases earlier than Release 12.0(26)S.

The ingress CoS includes a **set** command for the matched class: either a **police** command with a **set** command or a simple **set** command and either a **set-mpls** command or a **set-dscp** command.

Possible Workaround: Configure static ARPs.

- CSCef26543

Symptoms: A Cisco 12000 series line card may rate-limit process-switched packets to the GRP. This situation causes a ping to be lost when you perform a ping test to the local interface of the router.

Conditions: This symptom is observed when the interface is configured for HDLC, when the interface has a hard loop, and when the IP address of the interface is the destination of the ping. Because the interface is in the up/up state (looped) and functional, there should be no packet loss when you ping the interface at its own IP address.

Workaround: There is no workaround.

- CSCef30689

Symptoms: The AToM label holddown period is too short, and AToM traffic may be misdirected.

Conditions: AToM holds down its VC labels for 20 seconds before it releases them to the label manager. These labels are then available for allocation to other protocols or features such as LDP, TE, and MPLS VPNs. However, 20 seconds is not sufficient to guarantee that the AToM peer has properly deleted the entries and may cause AToM VC traffic to be misdirected by the protocol or features to which the freed AToM label is allocated.

Workaround: There is no workaround.

- CSCef35911

Symptoms: MPLS IAS traffic without labels is dropped at one ASBR when PPP encapsulation is configured between two ASBRs.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S1 and that functions as an ASBR. However, the symptom may be platform-independent and may also occur in other releases.

Workaround: Change the encapsulation to HDLC.

- CSCef43691

A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP “hard” error messages.
2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks.
3. Attacks that use ICMP “source quench” messages.

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml>.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected.

- CSCef51239

Symptoms: When the MPLS LDP Graceful Restart feature is enabled, when label distribution protocol (LDP)-targeted sessions are configured, and when you globally disable LDP by entering the **no mpls ip** command while a graceful restart-enabled session is recovering, LDP may not be shut down properly.

When you then re-enable LDP by entering the **mpls ip** command, LDP may not allocate and advertise local labels for certain prefixes. When this situation occurs, MPLS connectivity may be interrupted because the router does not advertise a local label for certain prefixes.

Conditions: This symptom is observed when targeted sessions are requested to support ATOM circuits and when the router runs Cisco IOS Release 12.2S, or a release that is based on Release 12.2S, that contains the fix for CSCed18355.

A list of the affected releases can be found at <http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCed18355>. Cisco IOS software releases not listed in the “First Fixed-in Version” field at this location are not affected.

Workaround: Clear the routes for the affected prefixes from the routing table by entering the **clear ip route EXEC** command. Note that the fix for this caveat is also integrated in Release 12.0S, 12.3, and 12.3T.

- CSCef56201

Symptoms: Multicast MAC rewrites are not updated, preventing multicast traffic from being switched.

Conditions: This symptom is observed when the VLAN encapsulation is changed, for example from dot1q to dot1q, from dot1q to QinQ, or from QinQ to dot1q.

Workaround: Enter the **clear ip mroute** command.

- CSCef61610

A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP “hard” error messages.
2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks.
3. Attacks that use ICMP “source quench” messages.

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml>.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected.

- CSCef61721

Symptoms: CEF may not be updated correctly with a route change.

Conditions: This symptom is observed when IPv6 BGP is configured and when a route changes from iBGP to eBGP or the other way around.

Workaround: Repopulate CEF with the correct forwarding information by entering the **clear ipv6 route ipv6-address** command.

- CSCef63272

Symptoms: A recursive static default route may not have an outgoing MPLS label, causing all packets to be dropped.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(9) but may also occur in other releases.

Workaround: Add a nonrecursive static route to the BGP next-hop.

- CSCef67840

Symptoms: When the CEF table consistency checker is configured to perform a passive scan check of tables of the line cards, the CEF table consistency checker may report false inconsistencies, which you can view in the output of the **show ip cef ip-address** command. The false inconsistencies may occur because of a race condition.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(27)S1.

If an inconsistency is reported for a recursive loadbalanced route for which the output interfaces for the next-hop IP address differ between the RP and line card, you can ignore this inconsistency because this information is not used during the forwarding process.

Workaround: Disable the CEF table consistency checker so that no passive scan check is performed of tables of the line cards.

- CSCef70566

Symptoms: After you have configured an ACL on a router to deny a traffic stream, traffic is shaped unexpectedly.

Conditions: This symptom is observed when the **no access-list** command fails while a nonvolatile generation (NVGEN) occurs.

Workaround: There is no workaround.

- CSCef77337

Symptoms: An IPv6 ACL is not properly applied to multiple interfaces.

Conditions: This symptom is observed on a Cisco 12000 series when an IPv6 ACL is applied to multiple interfaces (that is, four or more) and is modified to exceed layer 4 operating capabilities that can be supported in hardware.

Workaround: There is no workaround.

- CSCef82700

Symptoms: A 4-port Gigabit Ethernet (GE) line card generates TCAM errors when a large QoS configuration is applied. The following messages are generated:

```
%QM-2-TCAM_ERROR: TCAM pgm error(8): ACL Merge Failed
%QM-4-SW_SWITCH: Interface GigabitEthernet2/0 routed traffic will be software
switched in egress direction(s)
```

In addition, when you modify the policy map while it is still attached to the interface of the 4-port GE line card, the TCAM utilization goes up drastically; however, when you remove the policy map from the interface, the TCAM utilization is not brought back to zero.

Conditions: These symptoms are observed on a Cisco 12000 series when a child policy map with 75 or more customers is applied and when each child policy has at least 6 queues.

Workaround: Change the default merge algorithm to POD by entering the **hw-module slot slot-number reload** command for the slot in which the affected line card is installed.

Alternate Workaround: To avoid problems with the policy map modification, remove the service policy from the interface, modify the service policy, and reattach the service policy to the interface.

- CSCef85231

Symptoms: When SSO redundancy mode is configured and you enter the **no** form of the **mpls ldp neighbor targeted** command to deconfigure a previously configured command, the standby RP may reload. The symptom may also occur when you enter the **no** form of the **mpls ldp neighbor implicit-withdraw** command. For example, any of the following command sequences may cause the symptom to occur:

Example 1:

```
mpls ldp neighbor 10.0.0.1 targeted ldp
...
no mpls ldp neighbor 10.0.0.1 targeted ldp
```

Example 2:

```
mpls ldp neighbor 10.0.0.1 targeted ldp
...
no mpls ldp neighbor 10.0.0.1 implicit-withdraw
```

Conditions: This symptom is observed when the **mpls ldp neighbor targeted** command is configured and when the Label Distribution Protocol (LDP) is globally disabled. (By default, LDP is globally enabled, but it can be disabled by entering the **no mpls ip** global configuration command.) The symptom does not occur when other commands are configured for the specific neighbor, for example, if an MD5 password is configured for the neighbor as illustrated in the command sequence below:

```
no mpls ip
```

```
mpls ldp neighbor 10.0.0.1 targeted ldp
mpls ldp neighbor 10.0.0.1 password foo
no mpls ldp neighbor 10.0.0.1 targeted ldp
```

This symptom occurs in releases that integrate the fix for caveat CSCee12408. A list of the affected releases can be found at

<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCee12408>.

Workaround: Configure a password for the neighbor as shown in the Conditions above before you enter the **no** form of the **mpls ldp neighbor targeted** command or the **no** form of the **mpls ldp neighbor implicit-withdraw** command.

- CSCef85916

Symptoms: In a scaled L2VPN configuration, CPUHOG-related tracebacks may be generated on a CE router.

Conditions: This symptom is observed on a Cisco 12000 series that runs the c12kprp-p-mz image of Cisco IOS Release 12.0(30)S and that functions as a CE router.

Workaround: There is no workaround.

- CSCef89470

Symptoms: After you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on an active GE interface or after you reload the router while an GE interface is active, the correct ARP entry is missing from the interface.

Conditions: This symptom is observed on a Cisco 10000 series that runs a Cisco IOS release later than Release 12.0(23)S.

Workaround: There is no workaround.

- CSCef89562

Symptoms: An Engine 4+ EPA-GE/FE-BBRD line card reports “%TX192-3-PAM_MODULE” and “%TX192-3-PAM_PIM” errors, and the interfaces continue to flap with the following error message:

```
%GRPGE-6-INVALID_WORD: Interface GigabitEthernet15/1/0: Detected RX Invalid Word
```

When there is heavy traffic, the line card may crash without generating any crashinfo.

Conditions: These symptoms are observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(26)S3 or Release 12.0(27)S3.

Workaround: There is no workaround.

- CSCef90783

Symptoms: The output counter on the interface of a PE router that faces a P router generates almost twice the value that it should provide.

Conditions: This symptom is observed in the following MPLS topology in which Cisco 12000 series routers are connected via interfaces of Engine 3 line cards:

A CE router (CE1) connects to a PE router (PE1) that connects, in turn, to a P router. This P router connects to another PE router (PE2) that, in turn, connects to another CE (CE2) router.

The symptom occurs when a VRF ping is generated from PE1 to the VRF interface of PE2, that is, the interface that is connected to CE2. The output counter on PE2 generates incorrect values.

Workaround: There is no workaround.

- CSCef91170

Symptoms: A Cisco 12000 series that has a CHOC12/DS1 ISE line card that is configured for mVPN over multilink PPP may not maintain PIM neighbors over GRE tunnels.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(27)S2, 12.0(27)S3, or 12.0(28)S1.

Workaround: On the multilink interface, enter the following sequence of commands:

```
Router(config)# interface multil
Router(config-if)# no ip pim sparse-dense-mode
Router(config-if)# ip pim sparse-dense-mode
```

Doing so enables the PIM neighbor to come up across the GRE tunnel.

- CSCef91475

Symptoms: A CPUHOG situation may occur intermittently on a Cisco 12000 series, causing fabric pipes to be lost and all OSPF and BGP adjacencies to be dropped.

Conditions: This symptom is observed in PRP on a Cisco 12000 series router.

Workaround: There is no workaround. However, the symptom resolves itself.

- CSCef93354

Symptoms: When MLP and SSO are configured and interfaces in a multilink bundle flap, the secondary PRE does not handle this situation correctly. When a PRE switchover occurs, the MLP bundle may enter an inappropriate state.

Conditions: This symptom is observed on a Cisco 10000 series.

Workaround: There is no workaround. To recover from the symptom, reload the Cisco 10000 series.

- CSCef94525

Symptoms: A port adapter that is installed in a VIP or FlexWAN and that is configured with more than 38 multilink bundles may crash.

Conditions: This symptom is observed on a Cisco 7500 series and Cisco 7600 series when distributed CEF switching is disabled either through entering the **no ip cef distributed** command or through a FIB-DISABLE event.

Workaround: There is no workaround.

- CSCef96652

Symptoms: The offered rate counter in the output of the **show policy-map interface** command is inaccurate.

Conditions: This symptom is observed on a Cisco 12000 series when very high traffic rates are used.

Workaround: There is no workaround.

- CSCef97190

Symptoms: The “giants” counter increments continuously for a serial T1 interface when MR-APS is configured on a 4-port channelized STM-1 line card. The symptom occurs even when the fiber is pulled from the OC-3 port.

Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.3(7)X11 when the serial T1 interface is in the inactive state, irrespective of whether it is the working interface or the protect interface. The symptom does not occur when the serial T1 interface is in the active state, again irrespective of whether it is the working interface or the protect interface. The symptom may also occur in other releases.

Workaround: There is no workaround.

- CSCef97964

Symptoms: A VIP4-80 crashes when you enter the **redundancy force-switchover** command.

Conditions: This symptom is observed on a Cisco 7513 that runs Cisco IOS Release 12.0(28)S1 and that is configured for SSO.

Workaround: There is no workaround.

- CSCeg00111

Symptoms: Padded IP fragments with an IP length that is shorter than 64 bytes and the More Fragments (MF) (which is set to 1) are dropped by an Engine 4+ line card that functions as an egress line card.

Conditions: This symptom is observed when the ingress line card is an Engine 4+ DPT line card and the egress line card is any Engine 4+ line card.

Workaround: There is no workaround.

- CSCeg00338

Symptoms: A high CPU utilization may occur at the interrupt level on a Cisco 10000 series when CLNS traffic is forwarded.

Conditions: This symptom is observed on a Cisco 10000 series that is configured with an PRE-1 and that runs Cisco IOS Release 12.0(24)S6.

Workaround: There is no workaround.

- CSCeg02016

Symptoms: The OSPF process may be down for link-bundling subinterfaces.

Conditions: This symptom is observed on a Cisco 12000 series that is configured with two RPs and that runs Cisco IOS Release 12.0(30)S when the redundancy mode is set to SSO.

Workaround: Change the redundancy mode to RPR.

- CSCeg11513

Symptoms: When a Label Distribution Protocol (LDP) session flaps, error messages similar to the following may be generated:

```
TAGCON-3-PEERSM: TDP peer 10.1.3.55(172.16.1.1:0):
multiple deferred adjs

%TAGCON-3-PEERSM: TDP peer 10.1.3.54(172.17.1.1:0):
multiple deferred adjs
```

In most cases, these messages do not affect the LDP functions. However, when an Any Transport over MPLS (AToM) VC is configured over the LDP session, the AToM VC may stay in the down state.

Conditions: These symptoms are observed when Multiprotocol Label Switching (MPLS), LDP, and MLS LDP Graceful Restart are enabled.

Workaround: Disable MLS LDP Graceful Restart.

- CSCeg11773

Symptoms: The active RP crashes when you perform a microcode reload of the line cards while the standby RP is booting.

Conditions: This symptom is observed on a Cisco 12000 series that runs a Cisco IOS interim release for Release 12.0(30)S and that is configured for RPR.

Workaround: There is no workaround.

- CSCeg13308

Symptoms: An Engine 6 line card may reset when line card error recovery is invoked.

Conditions: This symptom is observed on a Cisco 12000 series router that runs the gsr-p-mz image of Cisco IOS Release 12.0(30)S.

Workaround: There is no workaround.

- CSCeg13868

Symptoms: When the **no tag-switching ip propagate-ttl** command is configured on PE routers and a traceroute is executed from one CE router to a remote CE router, an egress PE router replies to the traceroute with the address of its ingress MPLS interface.

Conditions: This symptom is observed only when the traceroute is destined for a network between an egress PE router and a remote CE router, when the ingress line card of the egress PE router is a Cisco 12000 series Engine 0 or Engine 1 line card.

Workaround: There is no workaround.

- CSCeg15191

Symptoms: An OC192E/POS-IR-SC line card resets with the following error messages:

```
%MBUS_SYS-3-NOBUFFER: Message from slot 3 in stream 1 dropped
```

```
%MDS-2-LC_FAILED_IPC_ACK: RP failed in getting Ack for IPC message of size 232 to LC in slot 3 with sequence 47350, error = timeout
```

```
%FIB-3-FIBDISABLE: Fatal error, slot 3: IPC Failure: timeout
```

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S1.

Workaround: There is no workaround.

- CSCeg19298

Symptoms: A router may crash when you enter the **show running-config** command.

Conditions: This symptom is observed when a bundle is configured on an ATM interface and when you enter the **show running-config** after you have entered the **no protocol protocol-address** command for the bundle.

Workaround: There is no workaround.

- CSCeg19635

Symptoms: The PXF engine on a Cisco 10000 series may crash, causing traffic through the router to be interrupted temporarily.

Conditions: This symptom is observed on a Cisco 10000 series when a security ACL is changed and immediately applied to an interface while traffic is traversing the interface. The symptom may occur on a Cisco 10000 series that is configured with either a PRE1 or a PRE2.

Workaround: Wait several seconds between updating the ACL and applying it to the interface.

- CSCeg20771

Symptoms: During intense interaction between the RP and line cards, the RP may crash because of a corruption. This symptom occurs when large numbers of VRFs are continuously created and deleted. However, the trigger for the symptom to occur could be caused by something else.

Conditions: This symptom is observed on a Cisco 12410 that is configured with about 100 VRFs and that runs Cisco IOS Release 12.0(27)S2, 12.0(28)S1, or an interim release for Release 12.0(29)S. The symptom is not observed in Release 12.0(30)S.

Workaround: Do not add or delete more than VRFs at one time.

- CSCeg25493

Symptoms: Several VIPs may crash at about the same time because of a bus error.

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(26)S4 and that is configured with an RSP4 when the VIPs are configured for QoS but have insufficient memory.

Workaround: Increase the amount of memory on the VIPs.

- CSCeg28402

Symptoms: Spurious memory accesses may occur on a Cisco 7500 series and may cause high CPU usage on the RSP.

Conditions: This symptom is observed on a Cisco 7500 series that is configured for distributed Multilink PPP (dMLP) and that functions in an MPLS network.

Note that packet switching for MPLS packets over MLP bundles is not supported at the RSP level in Cisco IOS Release 12.0S.

Workaround: There is no workaround.

Further Problem Description: The fix for this caveat causes packets that are sent to the RSP for switching to be dropped. Distributed forwarded packets are forwarded correctly.

- CSCeg29995

Symptoms: A router crashes when you create an IPv6 static neighbor entry that replaces an incomplete ND cache entry and when you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command multiple times on the interface that connect to the neighbor.

Conditions: This symptom is observed when the following events occur:

- 1) The router receives and attempts to forward packets to a non-responding IPv6 neighbor, causing the router's ND cache entry for the IPv6 neighbor to be in the incomplete (INCMPL) state.
- 2) You create a static neighbor entry by entering the **ipv6 neighbor** command for the same (non-responding) neighbor.
- 3) You enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command multiple times on the interface on which the static neighbor entry is defined, or the interface is shut down and the static neighbor is deleted.

Workaround: Ensure that the IPv6 static neighbor is manually created before the processing of traffic causes an incomplete ND cache entry to be created for the same neighbor.

- CSCeg30179

Symptoms: Removing a policy that has shape and bandwidth in the same class (in that same order) may cause a router to crash.

Conditions: This symptom is observed when the router functions under a traffic load.

Workaround: There is no workaround.

- CSCeg31912

Symptoms: Ingress policing and bandwidth percent per-class do not function and limit traffic at the configured bandwidth for MLFR links. The output of the **show policy-map interface** command shows the configured bandwidth which differs from the actual bandwidth.

Conditions: This symptom is observed on a Cisco 7500 series after the router is reloaded.

Workaround: Remove the service policy and re-apply it to interface to enable correct calculation of the interface bandwidth.

- CSCeg33229

Symptoms: A VIP may crash when an ingress service policy is removed from an MFR interface.

Conditions: This symptom is observed on a Cisco 7500 series while traffic is being processed on the MFR interface.

Workaround: There is no workaround.

- CSCeg37937

Symptoms: Non-initial fragments that may be part of a valid Layer 4 flow are denied and do not match the Layer 3 information. Normally, an ACE with Layer 3 and Layer 4 information will only match the Layer 3 information of non-initial fragments since the Layer 4 information is not available.

Non-initial fragments will only be permitted by explicitly using the *fragments* keyword.

Conditions: This symptom has been observed when a Cisco 12000 series router was performing IPv6 ACL filtering.

Workaround: There is no workaround.

- CSCeg44491

Symptoms: MFR Xconnect does not come up and the following error message and traceback are generated:

```
%SW_MGR-3-CM_ERROR: Connection Manager Error - unprovision segment failed  
[SSS:FR:356438] - no private context found.
```

```
-Traceback= 60FA8C28 60FA8D2C 6049715C 60FA6CC4 60FAF7D4 60FA6E70 60FA7050 60FA4DE0  
60FAF7D4 60FA5120 60FA2C84 60FA2CE4 60FA412C 60FA4394
```

Conditions: This symptom is observed on a non-distributed Cisco platform such as a Cisco 7200 series when you attempt to configure Xconnect on an MFR interface.

Workaround: There is no workaround.

- CSCeg45888

Symptoms: You cannot ping a global IPv6 address from a dual-mode IEEE 802.17 RPR/SRP uplink module.

Conditions: This symptom is observed on a Cisco 10720.

Workaround: There is no workaround.

- CSCeg66282

Symptoms: The controller of a 1-port multichannel STM-1 port adapter (PA-MC-STM1) does not come up after the router has reloaded.

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(28)S2.

Workaround: There is no workaround.

- CSCeg66627

Symptoms: An Engine 6 line card may reset because of an IPC timeout and may generate the following error message:

```
%MCC192-3-CPUIF_ERR: Packet Exceeds Programmed Length
```

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(27)S3.

Workaround: There is no workaround.

- CSCeg67495

Symptoms: A VIP may crash due to a bus error.

Conditions: This symptom has been observed in Cisco IOS Release 12.0(29)S.

Workaround: There is no workaround.
- CSCeg69381

Symptoms: When you perform a physical OIR or you reload microcode on a line card that is installed in slot 15, Engine 6 line cards in other slots of the chassis are reset and CEF failure messages are generated. This situation affects traffic and routing updates.

Conditions: The symptom is observed on a Cisco 12000 series. When you perform a physical OIR or you reload microcode on a line card that is installed in a slot other than slot 15, the symptom does not occur.

Workaround: There is no workaround.
- CSCeg74271

Symptoms: In some cases, when changing the IP address of the PGP link in an MR- APS configuration, the router may pause indefinitely.

Conditions: This symptom was observed on a Cisco 12000 router running Cisco IOS Release 12.0(30)S. This symptom also affects other Cisco router families running Cisco IOS Release 12.0(30)S.

Workaround: There is no workaround.
- CSCeg76331

Symptoms: There may be an incomplete adjacency on a PE router for the IP address of the Gigabit Ethernet interface of a locally-connected next-hop CE router and there may be an incomplete ARP entry for the next-hop CE router in the VRF ARP cache of the PE router.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(30)S, that functions as a PE router with static routes that are configured within the VRF, and that has a 4-port Gigabit Ethernet line card as the egress line card.

The symptom occurs when a packet is lost when traffic is sent from a remote CE or PE router and when you enter the **shutdown** command followed by the **no shutdown** command on the VRF interface of the Cisco 12000 series.

Workaround: From the Cisco 12000 series, ping the interface of the locally-connected next hop CE router. Doing so populates the ARP cache and enables the incomplete adjacency to become complete and valid.
- CSCeh00169

Symptoms: After you have reloaded a router, for each of the service policies that are attached to the interfaces of a 4-port OC-12 POS ISE line card, the policing of L2 VCs may fail when errors with the following associated error messages occur:

"Must remove existing service policy first .."

or

"Configured exceed actions are not supported when policing L2 VCs on interface.."

When the policing of L2 VCs fails, the following error message is generated:

"L2 policing config failed."

Conditions: This symptom is observed on a Cisco 12416 that runs the c12kprp-p-mz image of a Cisco IOS interim release for Release 12.0(31)S and that is configured with dual PRPs and 4-port OC-12 POS ISE line card that has a service policy attached to each of its interfaces.

Following are examples of configurations that may trigger the symptoms:

```
policy-map testing-input
  class class-default
    police cir percent 2 pir percent 4
    conform-action set-mpls-exp-imposition-transmit 4
    exceed-action set-mpls-exp-imposition-transmit 1
    violate-action drop
!
map-class frame-relay testing
  service-policy input testing-input

interface POS6/0
  frame-relay interface-dlci 17 switched
  class testing
```

Workaround: There is no workaround.

- CSCeh05594

Symptoms: A router configured for FRR crashed when the interface went down and FRR was triggered.

Conditions: This symptom was observed when running Cisco IOS Release 12.0(30)S.

Workaround: Upgrade the Cisco IOS from Cisco IOS Release 12.0(30)S.

- CSCeh08518

Symptoms: The over-subscription factor needs to be increased to configure more virtual channels (VC) and virtual paths (VP) on an ATM interface.

Conditions: This symptom occurs when Cisco IOS Release 12.0S is running on a Cisco 10000 series router.

Workaround: There is no workaround.

- CSCeh09448

Symptoms: The MR-APS Active interfaces continue to be active until the deadman timer expires. This results in traffic loss even though another interface on another router could take over for this MR-APS group.

Conditions: This symptom is observed when the router is reloaded.

Workaround: To prevent traffic loss, do a manual switchover before the router is reloaded.

- CSCeh11537

Symptoms: After a PRP switchover, the MDT tunnel to other PE routers may be torn down and does not come back up.

Conditions: This symptom is observed when a PRP switchover occurs on a Cisco 12000 series that functions as a PE router.

Workaround: Disable and re-enable the **mdt default group-address** command that is defined under the **ip vrf** command.

- CSCin65637

Symptoms: Latency is higher when priority queueing is configured for an interface of a 2-port Packet-over-SONET OC-3c/STM-1 port adapter (PA-POS-2OC3). Latency is higher even for priority packets.

Conditions: This symptom is observed when the data rate exceeds the OC-3 line rate and may occur on all types of VIPS on a Cisco 7500 series and on a Cisco 7200 series that is configured with an NPE-300, NPE-400, or NSE-1. The symptom does not occur on a Cisco 7200 series that is configured with an NPE-G1.

Workaround: To prevent the data rate from exceeding the OC-3 line rate, configure traffic shaping. This also brings the latency for priority packet to tolerable limits.

- CSCin67253

Symptoms: A Cisco 7500 series may stop forwarding traffic via an Any Transport over Multiprotocol Label Switching (AToM) virtual circuit (VC) that is configured on an 8-port multichannel T1/E1 PRI port adapter (PA-MC-8TE1+).

Conditions: This symptom is observed on a Cisco 7500 series that has a PA-MC-8TE1+ that is configured for Frame Relay over Multiprotocol Label Switching (FRoMPLS) or Frame Relay/ATM/Ethernet interworking when you perform an online insertion and removal (OIR) of the Versatile Interface Processor (VIP) in which the PA-MC-8TE1+ is installed.

Workaround: Remove and reconfigure the affected AToM VC.

- CSCin75746

Symptoms: When you perform an OIR of a PA-MC-8TE1 port adapter or you reload microcode onto the line card, the line card may generate the following error message and may stop forwarding traffic:

```
AC Switching: VIP Xmit failed: DLCI 426 context missing
```

Conditions: This symptom is observed on a Cisco 7500 series.

Workaround: There is no workaround. To re-enable the line card, enter the **tx-queue-limit** command on the affected interface of the line card.

- CSCin80743

Symptoms: Configurations of interfaces on a legacy interface processor such as an EIP or an FSIP on a Cisco 7500 series go down after a redundancy-forced switchover.

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(28)S or a later release or Release 12.2(25)S that is configured for SSO or RPR+.

Workaround: Manually reconfigure the interfaces.

- CSCin83445

Symptoms: Incoming multicast traffic on a distributed MLP link is process-switched.

Conditions: This symptom is observed on a Cisco 7500 series that is configured for distributed MLP after the router has been reloaded.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected multilink interface.

- CSCin84124

Symptoms: After performing a Fast Software Upgrade (FSU), none of the interfaces of the active RSP come up.

Conditions: This symptom is observed on a Cisco 7500 series after you have performed a FSU to Cisco IOS Release 12.2(25)S or Cisco IOS Release 12.0(30)S and after an SSO switchover has occurred.

Workaround: After the FSU, enter the **microcode reload** command.

- CSCin87776

Symptoms: Multilink bundles on a Cisco 7500 router may start doing process switching instead of dCEF. This will cause RSP CPU usage to shoot up and CPU hog of the RSP.

Conditions: This symptom is most likely to occur when a RPR+ switchover happens on an HA-configured Cisco 7500. This issue can also occur when the MLP Link flaps.

Workaround: There is no workaround.

Further Problem Description: This problem will not happen with an SSO switchover, because the MLP state is maintained (meaning the MLP interfaces will not flap). However, the problem still could be seen if the Links flaps due to some other reason.

- CSCin88417

Symptoms: Transmit accumulator loss may be seen for MLP interfaces after VIP OIR. MLP may stop forwarding or DCEF switching the packets if Transmit accumulator value goes to 0.

Conditions: This symptom has been observed on VIP OIR removal and insertion with traffic running on MLP bundles.

Workaround: Reload VIP again while making sure that no traffic is going out on the MLP bundles just immediately after VIP comes up.

- CSCsa42857

Symptoms: A duplex configuration (half/full) is not saved to NVRAM. This situation causes the default configuration (half duplex) to be used after the router reloads.

Conditions: This symptom is observed on a PA-2FE port adapter that is installed in a Cisco 7200 series that runs Cisco IOS Release 12.0(28)S1.

Workaround: There is no workaround.

- CSCsa46154

Symptoms: A Route Processor (RP) failover occurs.

Conditions: This symptom occurs when you enter the **show route-map** command in one session and remove several route maps in rapid succession in another session.

Workaround: Do not enter the **show route-map** command when you remove route maps in a concurrent vty session.

- CSCsa46699

Symptoms: A Cisco 7200 series may crash because of a bus error when you remove a subinterface or when you remove a service policy from an interface.

Conditions: This symptom is observed when a hierarchical policy map is configured, when the policy map has a police action in the child only, and when the policy map is attached to two interfaces. When the service policy is removed from one of the interfaces, the router may crash.

Workaround: Configure the same policy map with a different name on each interface.

- CSCsa46859

Symptoms: Cisco 10000 series routers using ATM VC bundles and QoS may have packets dropped when an external ATM VC bundle using DSCP type of service traverses the Cisco 10000.

Conditions: When using ATM VC bundles and Cisco IOS Release 12.0 S on a Cisco 10000 series router, ATM VC bundle traffic may be dropped. The problem arises when ATM bundles using DSCP enter the Cisco 10000 router which only supports MPLS EXP type of service bits. Those code points not matching an MPLS EXP TOS value exactly are dropped.

Workaround: Either use MPLS EXP for ATM bundles leading into the Cisco 10000 router or only use DSCP values that map to the MPLS EXP values.

- CSCsa46887

Symptoms: A router builds an Echo Reply that is invalid and may be misunderstood.

Conditions: This symptom is observed on a router that is configured for LSPV when the router receives an Echo Request with a Pad TLV that has a value of “Copy Pad TLV to reply.” The Echo Reply that the router builds includes residual data from previously received packets instead of the pad pattern that was received.

Workaround: There is no workaround.

- CSCsa47020

Symptoms: When Multilink Frame Relay (FRF.16) is configured on two bundled serial links and when the traffic rate is above 2 Mbps, packet loss occurs.

Conditions: This symptom is observed on a Cisco Catalyst 6500 series and a Cisco 7500 series when you send a 64-byte Ethernet frame. The symptom does not occur when the frame size is 512 bytes or more.

Workaround: There is no workaround.

- CSCsa56415

Symptoms: A router may pause indefinitely or reload unexpectedly.

Conditions: This symptom is observed while deleting or recreating policing access control lists (ACLs) or shaping ACLs via a script.

Workaround: Update the access control list (ACL) rather than delete it.

- CSCsa59002

Symptoms: IP fragments with a User Datagram Protocol (UDP) protocol identifier may be improperly denied on an Engine 3 line card that has an outbound access control list (ACL) that denies specific UDP ports.

Conditions: This symptom is observed only for outbound ACLs on an Engine 3 line card on a Cisco 12000 series. The following is an example of an ACL statement for which the symptom may occur:

```
access-list 100 deny udp any any eq 0 <<< this line may accidentally deny IP fragments
for UDP access-list 100 permit ip any any
```

Workaround: Use the following ACL instead of the above-mentioned example:

```
access-list 101 permit udp any any fragments
access-list 101 deny udp any any eq 0
access-list 101 permit ip any any
```

- CSCsa64782

Symptoms: When an ingress ISE line card is used with a default route that iBGP learns over a MPLS core, the following two symptoms may occur:

- The output of the **show controllers tofab alpha mip stat | i MTU** command may show traffic drops.
- Traffic is incorrectly sent as “unlabeled” over the MPLS core.

Conditions: These symptoms are observed on a Cisco 12000 series when the traffic path follows a recursive default route and when recursive load sharing occurs.

Workaround: Prevent outbound load sharing to the default route by changing the IGP metrics.

- CSCuk55561

Symptoms: A compact flash (CF) disk that is formatted in Cisco IOS-XR software does not mount on a platform that runs Cisco IOS software. The compact flash disk is successfully formatted from Cisco IOS-XR software, however, the **show compactflash: filesys** command reports the wrong device format.

Conditions: This symptom is observed when a compact flash disk that is formatted by Cisco IOS-XR software is used on a platform that runs Cisco IOS software.

Workaround: Format the disk using Cisco IOS.

- CSCuk55758

Symptoms: On Cisco 7500 series routers and Cisco Catalyst 6500 series switches with MSFC cards, distributed CEF does not automatically become enabled after issuing an **ip routing** command.

The output from the **show cef state** command shows that the distributed CEF state is “dCEF disabled/not running”, and the packet forwarding performance is very poor.

Conditions: This symptom is observed only in a Cisco IOS interim release for Cisco IOS Release 12.0(30)S and an interim release for Release 12.2S.

Workaround: Enable distributed CEF by using the **ip cef distributed** command.

TCP/IP Host-Mode Services

- CSCeg20351

Symptoms: An RR is unable to negotiate the optimal MSS with their MP-BGP neighbors.

Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.0(28)S1, that functions as an RR, and that has Path MTU Discovery (PMTUD) enabled. The symptom may also occur in other releases.

Workaround: There is no workaround.

Wide-Area Networking

- CSCsa49019

Symptoms: A memory leak may occur in the “Multilink Events” process, which can be seen in the output of the **show memory summary** command:

```
0x60BC47D0 0000000024 0000000157 0000003768 MLP bundle name
0x60BC47D0 0000000028 0000000003 0000000084 MLP bundle name
0x60BC47D0 0000000044 0000000001 0000000044 MLP bundle name
0x60BC47D0 0000000048 0000000001 0000000048 MLP bundle name
0x60BC47D0 0000000060 0000000001 0000000060 MLP bundle name
0x60BC47D0 0000000064 0000000013 0000000832 MLP bundle name
0x60BC47D0 0000000068 0000000008 0000000544 MLP bundle name
0x60BC47D0 0000000072 0000000001 0000000072 MLP bundle name
0x60BC47D0 0000000076 0000000001 0000000076 MLP bundle name
0x60BC47D0 0000000088 0000000018 0000001584 MLP bundle name
```

Conditions: This symptom is observed when two interfaces are configured in the same multilink group or are bound to the same dialer profile.

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.0(30)S

All the caveats listed in this section are resolved in Cisco IOS Release 12.0(30)S. This section describes only severity 1, severity 2, and select severity 3 caveats.

Basic System Services

- CSCed67358

Symptoms: An IPv6 PIM neighbor may be down after changing the PIM configuration.

Conditions: This symptom is observed when the **no ipv6 pim** command is entered on some subinterfaces of a physical Ethernet interface and when PIM is enabled on several subinterfaces of the same physical Ethernet interface. The symptom affects both IPv4 and IPv6, and configurations with multicast and OSPF Hello messages.

Workaround: There is no workaround.

- CSCee04316

Symptoms: A TN-2-BADCONN message may appear in the log and may be quickly followed by an FIB Disable message, indicating that distributed CEF is disabled on all VIPs. The IPC buffers usage may grows very large (up to 600 MB) and these buffers may not be reclaimed.

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(26)S1 and that has a very large BGP table and several VRFs.

Workaround: Reload the router to restore normal operation.

- CSCee78266

Symptoms: A Cisco 7500 series may reload in an indefinite loop when you unintentionally enter the **show list number** hidden command.

Conditions: This symptom is observed when you, for example, abbreviate the **show line 2000** command as the **show li 2000** command and actually execute the **show list 2000** hidden command.

Workaround: Do not abbreviate the **show line** command as the **show li** command but enter the full command.

- CSCee87891

Symptoms: SNMP entries may be deleted when you configure SNMP or when you reload the router on which SNMP is configured.

Conditions: This symptom is observed when an SNMP user is configured with the same name or host name as a community.

Workaround: There is no workaround.

- CSCee95282

Symptoms: A router may generate a very large remote processing time report that may take between 10 and 25 seconds to be generated.

Conditions: This symptom is observed when you enter the **rtr responder** command for the first time and you do not reload the router.

Workaround: Reload the router after you have entered the **rtr responder** command.

- CSCef15418

Symptoms: A router cannot write to Bootflash.

Conditions: This symptom is observed on a Cisco router after you have entered the **squeeze bootflash** command.

Workaround: There is no workaround.

- CSCef53395

Symptoms: A memory leak may occur in the IPC buffers of a Cisco router, and the output of the **show processes memory** command shows that the Pool Manager process holds increasingly more memory.

```
Router#show proc mem
```

```
Total: 231201504, Used: 202492916, Free: 28708588
```

PID	TTY	Allocated	Freed	Holding	Getbufs	Retbufs	Process
...							
5	0	149227592	69514888	79894996	135335724	66834832	Pool Manager

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(26)S2 or 12.0(26)S3. The memory leak is triggered by the SNMP polling of specific OIDs within the ciscoEnhancedMemPoolMIB MIB.

Workaround: Prevent the ciscoEnhancedMemPoolMIB MIB from being polled by explicitly configuring an SNMP view. To prevent this MIB from being accessed via any community strings, create a view and apply the view to all communities configured, as in the following example:

```
snmp-server view NOMEMPOOL iso included
snmp-server view NOMEMPOOL ciscoEnhancedMemPoolMIB excluded
snmp-server community public1 view NOMEMPOOL ro 6
snmp-server community public2 view NOMEMPOOL ro 7
snmp-server community public3 view NOMEMPOOL ro 8
```

The specific MIB that is being blocked is ciscoEnhancedMemPoolMIB (1.3.6.1.4.1.9.9.221).

Once the configuration is in place, the router must be reloaded to clear the IPC cache and free the memory.

- CSCin63066

Symptoms: When a new probe (for example, index \$PROBE_ID) is created through SNMP, the probes that have index numbers that are greater than \$PROBE_ID are not shown in the output of the **show rtr configuration** and **show rtr operation-state** commands.

Conditions: This symptom is observed when the probe is created in the CREATE_AND_WAIT state by entering the following command:

```
unix_xterm>
setany -v1 $ROUTERIP public
rttMonCtrlAdminStatus.$PROBE_ID 5
```

In addition, there is no subsequent SNMP configuration command for the probe.

Workaround: Enter a subsequent SNMP configuration command to make the probe configuration complete, as in the following example:

```
setany -v1 $ROUTERIP public \
rttMonCtrlAdminRttType.$PROBE_ID -i 1 \
rttMonEchoAdminProtocol.$PROBE_ID -i 2 \
rttMonEchoAdminTargetAddress.$PROBE_ID -o "05 00 00 02"
```

- CSCin78428

Symptoms: A router crashes when you enter the **snmp-server host** command.

Conditions: This symptom is platform-independent.

Workaround: There is no workaround.

Interfaces and Bridging

- CSCee25605

Symptoms: When you enter the **show ip interface brief**, the output indicates that a serial subinterface has a down status and that the protocol is down too:

```
router# show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Ethernet0/0	10.7.0.68	YES	NVRAM	up	up
Ethernet0/1	unassigned	YES	NVRAM	administratively down	down
Ethernet0/2	unassigned	YES	NVRAM	administratively down	down
Ethernet0/3	unassigned	YES	NVRAM	administratively down	down
Ethernet0/4	unassigned	YES	NVRAM	administratively down	down
Ethernet0/5	unassigned	YES	NVRAM	administratively down	down
Serial4/0	unassigned	YES	NVRAM	administratively down	down
Serial4/1	unassigned	YES	NVRAM	administratively down	down
Serial4/2	unassigned	YES	NVRAM	administratively down	down
Serial4/3	unassigned	YES	NVRAM	administratively down	down
Serial4/4	unassigned	YES	NVRAM	administratively down	down
Serial4/5	unassigned	YES	NVRAM	administratively down	down
Serial4/6	unassigned	YES	NVRAM	administratively down	down
Serial4/7	unassigned	YES	NVRAM	administratively down	down
Serial5/0:23	10.0.0.1	YES	NVRAM	down	down

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(26)S1 when you attempt to configure the interface and bring it up.

Workaround: There is no workaround.

- CSCee44827

Symptoms: Spurious memory accesses may occur on a VIP with a PA-FE.

Conditions: This symptom is observed on a Cisco 7500 series when a raw Ethernet packet is received on the PA-FE interface that is configured as an ISL trunk.

Workaround: There is no workaround.

IP Routing Protocols

- CSCec22723

Symptoms: A router may unexpectedly reload because of a watchdog timeout or bus error in OSPF.

Conditions: This symptom is observed when iSPF is configured under OSPF.

Workaround: Remove the iSPF configuration from OSPF by entering the **no ispf** command.

- CSCee43166

Symptoms: The BGP inbound update processing becomes slow and a high CPU utilization occurs for a long time.

Conditions: This symptom is observed when a large number of VRFs (more than 200) and prefixes (more than 220,000) are configured.

Workaround: There is no workaround.
- CSCee66936

Symptoms: A software-forced reload may occur on a router that is configured with a DVMRP tunnel.

Conditions: This symptom is observed on a Cisco router when the DVMRP tunnel is brought up and routing information is redistributed between DVMRP and MBGP.

Workaround: There is no workaround.
- CSCee85676

Symptoms: When VPNv4 route advertisement are received after BGP has converged, the existing path is updated but imported paths from the original path are not updated accordingly.

Conditions: This symptom is observed on a Cisco router that functions as a PE router when the **maximum-paths number-of-paths import number-of-paths** command is enabled. The symptom occurs when the path attributes are changed dynamically instead of the path being completely withdrawn and readvertised.

Workaround: Withdraw the prefix from the remote PE router and then readvertise the prefix.
- CSCee86530

Symptoms: A BGP update that is sent to a connected P router fails to report the martian next-hop log message when the next-hop field in the attribute of the BGP update is set to 255.255.255.255 (that is, all 1s). The P router does deny the advertisement of the MP_REACH_NLRI attribute to the other PE routers, but there is no log message to indicate that it is denying the advertisement and why it does so.

Conditions: This symptom is observed during MP-BGP negative testing for the MP_REACH attribute.

Workaround: There is no workaround.
- CSCee88542

Symptoms: A Cisco router may reload unexpectedly when you enter the **show ip msdp peer** command.

Conditions: This symptom is observed when the MSDP session flaps while you enter the **show ip msdp peer** command.

Workaround: There is no workaround.
- CSCee89438

Symptoms: An MSDP enabled RP does not build an (S,G) state from its SA cache when it should do so. Depending on the topology and if an SPT threshold is configured as infinite, this situation may result in a multicast forwarding interruption of up to 2 minutes.

Conditions: This symptom is observed when the RP for a group fails and an incoming (*,G) join message is received.

MSDP should create an (S,G) state from its SA cache. However, this is done before the (*,G) olist is populated; because of the (*,G) NULL olist, MSDP does not install an (S,G) state.

Workaround: Enter the **clear ip mroute *** command on all first-hop routers to the source to enable the FHR to register immediately when the next packet creates an (S,G) state.

- CSCee94020

Symptoms: The **timer** command to configure SPF and LSA may not be available.

Conditions: This symptom is observed when the OSPF VRF process is configured.

Workaround: There is no workaround.

- CSCef00296

Symptoms: A router crashes when you remove the peer-group members.

Conditions: This symptom is observed on a Cisco router that is configured for BGP.

Workaround: There is no workaround.

- CSCef00535

Symptoms: An OSPF router may reload unexpectedly.

Conditions: This symptom is observed after a neighbor has performed a switchover.

Workaround: Disable LLS under the OSPF process on the router by entering the **no capability lls** command or disable OSPF NSF under the OSPF process on the neighbor by entering the **no nsf** command.

- CSCef08797

Symptoms: A router may stop redistributing static routes into BGP.

Conditions: This symptom is observed when the static routes are inserted into the BGP table with a network statement that uses a route map that is configured with the **match as-path** route-map configuration command.

The symptom occurs because the **match as-path** route-map configuration command causes a non-BGP route to be denied.

Workaround: Do not use BGP-specific match statements when you source non-BGP routes.

- CSCef17311

Symptoms: An %ALIGN-3-SPURIOUS error message and a traceback may be generated when you configure BGP and MPLS VPN.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.3(9.10)T but may also occur in other releases such as Release 12.0 S and Release 12.2 S.

Workaround: There is no workaround

- CSCef34586

Symptoms: BGP IPv4 label session continue to flap after an interface between two EBGp peers flaps.

Conditions: This symptom is observed when EBGp IPv4 with labels is configured between two BGP peers. The session comes up fine the first time after you reload one of the BGP peers. After you toggle an interface between the BGP peers, the EBGp session continues to flap because of malformed updates.

Workaround: There is no workaround.

- CSCef64928

Symptoms: The output of the **show bgp ipv6 neighbors ipv6-address | b ly: ipv6 unicast** command does not show the peer information. The output provides “BGP IPv6” instead of “IPv6 Unicast” information. However, this is just a display problem and the functionality is not affected.

Conditions: This symptom is observed on a Cisco 7200 series that runs the c7200-js-mz image of Cisco IOS interim Release 12.3(10.3)T3. However, the symptom may not be platform-dependent.

Workaround: There is no workaround.

- CSCef81489

Symptoms: If an ASBR receives a withdraw message, it does not send the withdraw message to any peer, preventing an alternate route from functioning.

Conditions: This symptom is observed when MPLS VPN inter-AS is configured.

Workaround: There is no workaround. To recover from the symptom, enter the **clear ip bgp *** command on the ASBR.

ISO CLNS

- CSCef30864

Symptoms: You may not be able to ping a router using the CLNS protocol via Frame Relay encapsulation.

Conditions: This symptom is observed when the **encapsulation frame-relay** command is enabled.

Workaround: There is no workaround.

- CSCef70231

Symptoms: When you enter the **no clns routing** command, adjacencies may be lost on any interface that is configured for IS-IS.

Conditions: This symptom is observed on a router that is configured for IS-IS and CLNS only when IS-IS is not specifically configured to route CLNS.

Workaround: Do not enter the **no clns routing** command when IS-IS is not specifically configured to route CLNS.

- CSCuk52227

Symptoms: A router unexpectedly reloads when you show the running configuration or you save the configuration to NVRAM.

Conditions: This symptom is observed on a Cisco router when the **redistribute static clns route-map map-name** command is enabled as part of the configuration of the **router isis** command.

Workaround: Enable the **redistribute static clns** command without the **route-map** keyword and the **map-name** argument.

Miscellaneous

- CSCea26450

Symptoms: Under rare circumstances, an Operation, Administration, and Maintenance (OAM)-enabled ATM Permanent Virtual Circuit (PVC) may stay in the down state.

Conditions: This symptom is observed when the ATM interface transitions to the down state and then back to the up state because of a-link related problem or because you enter the **shutdown** command followed by the **no shutdown** command.

Workaround: Disable OAM on the PVC.

- CSCeb31767

Symptoms: A flash disk or compact flash disks may not be recognized.

Conditions: This symptom is observed when a new flash disk or compact flash disk (that has not been formatted earlier on a platform that runs Microsoft Windows 95 or 98) is formatted on a platform that runs Microsoft Windows 2000.

Workaround: There is no workaround.

- CSCeb52181

Symptoms: A Cisco platform that accesses the “system:/vfiles/tmstats_ascii” virtual file (for example, via “more system:/vfiles/tmstats_ascii”) may crash because of bus error.

Conditions: This symptom is observed under normal working conditions when no configuration changes are made on a Cisco platform that runs Cisco IOS Release 12.0 S, 12.1 E, 12.2 or 12.3. When the “system:/vfiles/tmstats_ascii” virtual file is not used, the symptom does not occur.

Workaround: There is no workaround.

- CSCeb78575

Symptoms: PRP may generate a program (0x700) or data storage (0x300) exception while booting an image from an ATA disk or PCMCIA card.

Conditions: This symptom is observed on a Cisco 12000 series PRP after repeated reloads.

Workaround: Reset the ROMmon.

- CSCec15517

Symptoms: A Cisco router may reload when you enter the **show policy-map interface** command in one router session while deleting the sub-interface on which the policy is attached from another session.

Conditions: This symptom is observed on a Cisco 7500 series that is configured with a Frame Relay permanent virtual circuit (PVC) policy.

Workaround: There is no workaround.

- CSCec64382

Symptoms: You may not be able to send traffic through an IPv6-to-IPv4 (6to4) tunnel, but you may be able to receive traffic through this tunnel.

Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.2 S or Release 12.3 when the interface on which the tunnel is configured flaps.

Workaround: There is no workaround.

- CSCec81075

Symptoms: You may be unable to pass traffic between an E3 interface on a Cisco 7304 router and an E3/T3 interface on a Cisco 10000 series router.

Conditions: This problem is seen when using the default DSU mode and the minimum bandwidth.

Workaround: Use another DSU mode, or set the bandwidth to something other than the minimum allowed.

- CSCec82589

Symptoms: After entering a **no hw-module slot** command on the primary CSC, an Engine 0 OC-12 (channelized to DS3) line card may become inoperable.

Conditions: This symptom is observed on a Cisco 12416 router that is running the gsr-p-mz image of Cisco IOS Release 12.0(24)S.

Workaround: Use the **microcode reload** global configuration command to reload the line card.

- CSCec87006

Symptoms: A Multilink PPP (MLP) interface on an Engine 3 CHoC12/T1 line card fails to accept an MQC policy that has a police CIR rate of more than 1536000 bps on the priority queue, even when the MLP interface has a bandwidth of 12288 kbps.

Conditions: This symptom is observed on a Cisco 12000 series router.

Workaround: There is no workaround.

- CSCed02844

Symptoms: IPv6 adjacencies may appear as incomplete, and connectivity may be broken. This situation occurs at random times and is not associated with any event in particular. IPv4 adjacencies may appear as incomplete but recover within a minute.

Conditions: This symptom is observed on a Cisco IOS-based router when you enter the **clear adjacency** command.

Workaround: To restore the correct state of the adjacency, enter the **shutdown** command followed by the **no shutdown** command on the affected interface.

- CSCed08168

Symptoms: No SNMP linkup or linkdown trap is generated for a 1CHOC12/4CHSTM1 SONET layer when a controller goes up and down.

Conditions: This symptom is observed when monitoring a SNMP linkup or linkdown trap for a 1CHOC12/4CHSTM1 SONET layer.

Workaround: Monitor the controller status using the **show controller sonet** command.

- CSCed13322

Symptoms: In the **show process memory** command output, the display of total and free memory may show more memory than is actually present in the main processor memory of the router. This is due to an undocumented change in the command output that also includes both processors and I/O memory pools in the amounts allocated by each process and the totals at the top of the output.

Conditions: This symptom is observed on all Cisco IOS platforms.

Workaround: Use the output of the **show memory summary** command to determine the individual amounts of total and free memory in each of the processor memory pools and the I/O memory pool.

- CSCed16318

Symptoms: When changing the MTU on an Engine 2 3-port 1GE line card, the line card may reload.

Conditions: This symptom is observed on a Cisco 12416 router that is running the gsr-p-mz image of Cisco IOS Release 12.0(26)S.

Workaround: Ensure there is no traffic going through the Engine 2 3-port 1GE line card when attempting to change the MTU.

- CSCed20839

Symptoms: After an interface flaps or when you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on an interface that is configured for Hot Standby Router Protocol (HSRP), a virtual HSRP address may not respond to pings.

Conditions: This symptom is observed on a Cisco router that is configured with a 2-port Fast Ethernet Inter-Switch Link (ISL) port adapter (PA-2FEISL) that has at least one Fast Ethernet interface configured for HSRP.

The symptom occurs because the Fast Ethernet interface that is configured for HSRP is not switched to promiscuous mode when the HSRP group becomes active, preventing packets that are addressed to the HSRP virtual MAC address from being received by the interface. The output of the **show controllers fastethernet** user EXEC or privileged EXEC command displays whether the promiscuous mode is enabled or disabled.

Reboot the router to restore the router to proper operation.

Workaround: To prevent the symptom from occurring, enter the **standby use-bia** interface configuration command on the Fast Ethernet interface that is configured for HSRP.

Further Problem Description: This caveat only effects Fast Ethernet port adapters and network modules that use the AMDP2 chipset (for example, the PA-2FEISL). When you use such a port adapter or network module with HSRP configured and the interface goes down, HSRP does no longer function when the interface comes back up.

- CSCed22303

Symptoms: The interface on an Engine 3 line card is stuck after hours of testing. When incoming packets are ignored, PPP does not go up.

Conditions: This symptom is observed on Cisco 12000 series router after hours of testing with an attenuator.

Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the affected interface.

- CSCed22358

Symptoms: A Cisco 12000 series may forward packets to an incorrect interface. This behavior can be seen by looking at the hardware CEF entry on this input line card:

```
execute-on slot x show ip hardware-cef a.b.c.d
(a.b.c.d is the destination IP address)
```

The output looks similar to the following, in which the CEF lookup is null:

```
LC-Slot0#show ip hardware-cef a.b.c.d
Leaf FCR 2 0x784C6FC0 found 2 deep
alpha ip loadbalance: 0x78198D00 - lbl not equal. cef lookup NULL
```

After clearing the route, the output looks as follows:

```
LC-Slot0#show ip hardware-cef a.b.c.d
Leaf FCR 4 0x784C6FC0 found 2 deep
Fast Adjacency:
alpha adjacency: 0x701E8280
[0-7] oi 0x4019100 oq 4000 in 15 ab 0 hl 20 gp 11 tl 0 loq BC01 15/0 mtu 4470
packets 1750013440 bytes 776867999767

Output Queue / Local Output Queue Bundle:
[0-7] output queue 0x4000 local output queue 0xBC01
```

This problem may cause packets to be dropped because a loop is created and the TTL expires for the packets.

Conditions: This symptom is observed under very specific conditions on a Cisco 12000 series that runs Cisco IOS Release 12.0(24)S or a later release when traffic that enters an Engine 3 line card toggles between a static-to-null route and a more specific route as the destination.

Workaround: Avoid the specific conditions mentioned above. Clearing the route resolves the problem only temporarily.

- CSCed47560

Symptoms: The native Gigabit Ethernet ports of a Cisco 7200 series NPE-G1 or a Cisco 7301 may stop forwarding traffic.

Conditions: This symptom is observed in a stress situation when bursty traffic is received.

Workaround: There is no workaround.

- CSCed54080

Symptoms: Per-VPN per-destination loadbalancing does not operate correctly on an Engine 2 or 4+ and there seems to be loadsharing only on BGP nexthop.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(23)S4.

Workaround: The **clear ip route vrf vrf-name** command invokes a recalculation of the hashes. Also, the **clear ip bgp neighbor soft** command (can) reassign(s) new labels and respread(s) the load. These commands may impact service by stopping traffic forwarding.

- CSCed55201

Symptoms: A serial interface may stop transmitting, and the following error message may be generated:

```
%RSP-3-RESTART: interface Serial1/0/2, not transmitting  
-Traceback= 403D8D88 403E2830 4036B72C 4036B718
```

Conditions: This symptom is observed on a Cisco 7500 series that is configured with an 8-port serial V.35 port adapter (PA-8T-V35).

Workaround for HDLC interfaces: Disable CDP, the passive interface, and the outbound IP ACL.

Workaround for Frame Relay interfaces: Disable CDP, the passive interface, the outbound IP ACL, and LMI.

- CSCed63508

Symptoms: Up to 10 percent of packets that are larger than 1496 bytes are dropped when passing through an Engine 3 4-port GE line card (4GE-SFP-LC).

Conditions: This symptom is observed on a Cisco 12000 series when the line card is used for both the ingress and egress traffic flow. This situation occurs when SNF is configured on the egress interface of the affected line card by entering the **ip route-cache flow sampled output** command.

Workaround: Increase the MTU on any interface of the Engine 4-port GE line card to 1530 bytes to enable the buffer resources of the line card to be initialized with a larger size.

Alternate Workaround: Decrease the rate of packets drops by increasing the sampling period. For example, when you enter the **ip flow-sampling-mode packet-interval 10** command, up to 10 percent of packets that are larger than 1496 bytes are dropped. However, when you enter the **ip flow-sampling-mode packet-interval 1000** command, only 0.1 percent of packets that are larger than 1496 bytes are dropped.

- CSCed64702

Symptoms: On a Cisco 10000 series, the PXF information may not be correctly updated from the RP after a route change, causing packets to be sent untagged even though the RP shows that the packets should be sent as tagged.

Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.0(26)S.

Workaround: Enter the **clear isis *** command or enter the **shutdown** command followed by the **no shutdown** command on the interface towards the MPLS cloud.

- CSCed67734

Symptoms: Packet processing at the remote end of a link may fail.

Conditions: This symptom is observed when a service policy that includes the **set atm-clp** command is enabled on an output interface via the **service-policy output** command; the platform that links to this output interface at the remote end drops the packets.

Workaround: Remove the **set atm-clp** command from the service policy on the output interface.

- CSCed69856

Symptoms: A Cisco 10000 series router may crash when access control lists (ACLs) are displayed.

Conditions: The symptom is observed when ACLs are displayed by entering the **show access-list** command just after an ACL has been added, deleted or modified. The probability of the crash increases with the size of the ACL and with the number of times it is used (for example, in route maps).

Workaround: Wait for a few minutes after modifying the ACL. For large size ACLs (with hundreds of entries) that is used many times you may have to wait between 5 and 10 minutes.

- CSCed70822

Symptoms: With four fabric cards (one CSC in slot 16 and three SFCs), after a power cycle, the line cards fail to come up and fabric ping timeouts occur.

Conditions: This symptom is observed on a Cisco 12000 series and affects all E4 and E4+ cards.

Workaround: Place a CSC card in slot 17. The fix for this caveat applies to all types of line cards (E0, E2, E3, E4 and E4+).

- CSCed72686

Symptoms: An ACL applied to an ATM subinterface (RFC1483) may not work after a PRE switchover.

Conditions: This problem is observed on a Cisco 10008 router with PRE2.

Workaround: Deconfigure and configure again the access list that is not working.

- CSCed74917

Symptoms: An ACL applied to a subinterface may become active on the main interface, without showing this in the configuration.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(25)S2.

Workaround: Do not apply the ACL to the subinterface.

- CSCed74933

Symptoms: A Cisco 12000 series may exhibit high CPU utilization in the “Per-Second Job” process.

Conditions: This symptom is observed on a Cisco 12012 router that has a GRP and that is running Cisco IOS Release 12.0(26)S1 with 255 class maps applied to a 4-port ISE Gigabit Ethernet line card. However, the symptom is release- and platform-independent.

Workaround: Reduce the number of applied class maps.

- CSCed76910

Symptoms: A CHOC12DS1 line card does not support a sufficient number of BERT patterns.

Conditions: This symptom is observed on a Cisco 12000 series.

Workaround: There is no workaround.

- CSCed78847

Symptoms: Cisco Express Forwarding (CEF) becomes disabled on a secondary Cisco 10000 series Performance Routing Engine (PRE) during a switchover.

Symptoms: This symptom is observed after configuring 380 traffic engineering (TE) tunnels and checking that CEF is enabled on both the primary and secondary PREs and that all TE tunnel interfaces are up. Then, a forced switchover from the primary PRE to the secondary PRE is performed. When the secondary PRE comes up and it now the new primary PRE, all tunnel interfaces are down. The line is up but the protocol is down. Because CEF is disabled and not running, the tunnels do not function and no routing can occur.

Workaround: Enable CEF on the primary PRE and enter the **shutdown** command followed by the **no shutdown** command on the affected interfaces. Doing so enables the TE tunnels to come up.

- CSCed79218

Symptoms: A Cisco 7200 series router with a PA-2CT3+ or PA-CT3 port adapter does not provide the configured minimum bandwidth guarantees.

Conditions: This behavior appears to be limited to the multichannel T3 family of port adapters and appears consistently upon the configuration of CBWFQ.

Workaround: There is no workaround.

- CSCed82152

Symptoms: An Engine 4+ line card may reset and generate errors.

Conditions: This symptom is observed after a manual RP switchover in RPR mode.

Workaround: There is no workaround.

- CSCed82592

Symptoms: A PXF engine on a Cisco 10000 series may unexpectedly crash and then the router may crash.

Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.0(23)S5.

Workaround: There is no workaround.

- CSCed82964

Symptoms: L2 loadbalancing might be affected on an egress link bundle.

Conditions: This symptom is observed a Cisco 12000 series when the ingress interface is a regular Engine 2 interface and when the member interfaces in the bundle are toggled.

Workaround: Enter the config mode of the port channel and exit.

- CSCed83129

Symptoms: A line card may crash when a router forwards multicast traffic in an MVPN environment.

Conditions: This symptom is observed when the data multicast distribution tree (MDT) advertisements that were received by the router expire. This situation causes the router to stop decapsulating packets in the VRF context and causes the router to send packets only from the interfaces that are defined in the global table.

Workaround: There is no workaround.

- CSCed84331

Symptoms: MPLS TE tunnel counters are inaccurate; the MPLS TE tunnel output rate counters may exceed the physical interface capabilities that the tunnel uses.

Conditions: This symptom is seen on a Cisco 12000 series that runs Cisco IOS Release 12.0(23)S5 with an Engine 4 line card. This symptom may be observed by issuing the following commands in the following order:

1. Enter the **show interfaces tunnel** *number* command. This command tells you the interface statistics for the tunnel.
2. Enter the **show mpls traffic-eng tunnels** *tunnel-interface* command. This command tells you the physical interface the tunnel traverses.
3. Enter the **show interfaces** *type slot/port* command. This command tells you the physical interface statistics.

Workaround: There is no workaround.

- CSCed84474

Symptoms: After an APS switch using channelized OC-12 line cards (channelized to DS-1), some Frame Relay interfaces may fail to carry traffic.

Conditions: This symptom is observed on a Cisco 12000 series with an OC-12 line card (channelized to DS-1) with a linear APS configuration.

Workaround: If an individual interface does not recover on its own, enter the **shutdown** command followed by the **no shutdown** command on the affected interface.

- CSCed89963

Symptoms: A Cisco 12000 series may experience a block overrun and redzone corruption with a subsequent system reload or switchover as a result of incorrectly processing a corrupted packet. Error messages similar to the following may be observed:

```
%GRP-4-CORRUPT: Corrupted packet, start_offset 96, length 65534, slot 9
%SYS-3-OVERRUN: Block overrun at 53E4389C (red zone 00000000)
```

Conditions: This symptom may be observed on a Cisco 12000 series that runs Cisco IOS Release 12.0 S and that has 1, 3, or 4 port Gigabit Ethernet line cards installed.

Workaround: There is no workaround.

- CSCed95753

Symptoms: A GRE tunnel may not work on a PE router.

Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of Cisco IOS Release 12.0(25)S or a later release.

Workaround: There is no workaround.

- CSCee00648

Symptoms: Engine 1 GE and FE line cards on a Cisco 12000 series running Cisco IOS Release 12.0(26)S2 may reset or fail when an HA switchover occurs.

Conditions: This symptom is observed when switching the HA mode from SSO to RPR+ or from RPR+ to SSO and when a test crash or switchover is performed while auto negotiation is enabled on the Engine 1 GE or FE line cards.

Workaround: Do not change the HA mode.

- CSCee01371

Symptoms: A ping to a local router interface may fail if the **ip source-track** command is configured for the IP address of the local router interface.

Conditions: This symptom is observed on a Cisco 12000 series Engine 0, Engine 2, and Engine 3 line card. Following is an example:

Router 1/0 (10.1.1.1) connects to Router 2/0 (10.1.1.2). After entering the **ip source-track 1.1.1.2** command on Router 2/0, ping 10.1.1.2 from Router 1/0 to Router 2/0 fails.

Workaround: There is no workaround.

- CSCee04454

Symptoms: A Cisco 10000 series router reloads unexpectedly as ATM VCs are coming up.

Conditions: This symptom is believed to occur only when ACLs are applied on ATM interfaces, and, only rarely then, on images that contain the CSCed72686 fix.

Workaround: There is no workaround.

- CSCee05549

Symptoms: A Label Switch Controller (LSC) may reload unexpectedly with a software-forced crash. An error similar to this one followed by a traceback can be seen:

```
%SYS-2-BADSHARE: Bad refcount in mem_lock, ptr=628371F8, count=0
```

Conditions: This symptom is observed when you enter the **show mpls atm-ldp bindings path** command to display LVC path information while network changes such as interfaces flaps or prefix flaps are occurring.

Workaround: There is no workaround.

- CSCee14179

Symptoms: When applied to a multilink PPP (bundle) interface, the **service-policy** command results in the following error message on the standby PRE:

```
CEF switching is required for the set command.
```

In addition, the multilink PPP interface configuration on the standby PRE indicates that there is no service policy on the interface.

Conditions: This symptom occurs only on multilink PPP (bundle) interfaces and only if the policy map referenced in the **service-policy** command contains a **set** command.

Workaround: The problem can be avoided by replacing the **set** command by a **police** command whose conform, exceed, and violate actions use the same action as in the **set** command. For example, if the **set** command is **set mpls experimental 5**, the equivalent **police** command is **police 8000 1000 0 conform-action set-mpls-exp-transmit 5 exceed-action set-mpls-exp-transmit 5 violate-action set-mpls-exp-transmit 5**.

- CSCee14817

Symptoms: HSRP over the VRF is not working after following these steps:

1. PE router 1 is the active HSRP router and a redundancy forced switchover occurs on PE router 2 (standby HSRP VPN) with SSO configured.
2. You enter the **shutdown** command on the GE subinterface of PE router 1.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(25)S3, that has a PRP and 4-port GE ISE line cards, and that functions as a PE router.

Workaround: Enter the **standby use-bia** command or use RPR+ instead of SSO.

- CSCee14840

Symptoms: A Cisco 12000 series running Cisco IOS Release 12.0(26)S1 may advertise erroneous IPv6 networks when configured for both 6PE and Route Reflector operation.

Conditions: This symptom is observed on a network in which 6PE is implemented on an existing dual-stack (IPv4 and IPv6) configuration.

Workaround: There is no workaround.

- CSCee16725

Symptoms: MPLS VPN VRF labels fail to be updated onto core-facing line cards such that the VPN traffic entering the core-facing line cards is punted to the RP.

Conditions: This symptom is observed in a setup with two parallel paths between a PE router and a CE router that run Cisco IOS Release 12.0 S. There are around 10,000 VRF routes advertised through both the eBGP sessions that are established between the PE router and the CE router. When the link flaps, the next hop of all the BGP routes changes to the next hop via the other link. When this situation occurs, the core-facing line cards may miss the label forwarding entry for some of the VPN prefixes.

Workaround: To recover from the problem after it has occurred, enter the **clear cef linecard** command on the affected core-facing line card.

To avoid the problem from occurring, do not redistribute the PE-CE link subnet into BGP.

- CSCee16950

Symptoms: IPv6 traffic forwarding on an Engine 2 DPT line card is performed by the CPU of the line card; IS-IS, OSPFv2 or OSPFv3 adjacencies, or BGP neighbourships across any of the interfaces of the Engine 2 DPT line card may fail.

Conditions: This symptom is observed when oversubscribing the CPU of the Engine 2 DPT line card in terms of its maximum IPv6 packet-per-second forwarding rate, which is about 100 Kpps.

Workaround: There is no workaround. The symptom does not occur for POS and GE Engine 2 line cards.

- CSCee18844

Symptoms: Traffic forwarding problems may occur when sending MVPN traffic from multiple sources to the same group.

Conditions: This symptom is observed on a Cisco 12000 series that functions as an MVPN decapsulation PE router with an Engine 3 line card that forwards multicast packets on a VRF interface.

Workaround: To ensure that no collisions occur on the VRF interface, configure hardware multicast on the Engine 3 line card by entering the **hw-module slot *number* ip multicast hw-accelerate source-table size *x* offset *y*** command.

- CSCee18883

Symptoms: All VIPs in a Cisco 7500 series restart as a consequence of a Cbus complex that is triggered by a stuck output. Just before the output becomes stuck, IPC timeout errors occur.

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.3(5) in a dLFloATM environment. The symptom may also occur in other releases.

Workaround: There is no workaround.

- CSCee18889

Symptoms: If link bundling is configured on any line card in the router and the link bundle is loaded onto an Engine 2 line card that has VPN on FR subinterfaces and that is processing traffic, the Engine 2 line card may reload.

Conditions: This symptom is observed on a Cisco 12000 series that is running the gsr-p-mz image of Cisco IOS Release 12.0(28)S.

Workaround: There is no workaround.

- CSCee19419

Symptoms: When link bundling is configured and you reload microcode onto a line card, the link bundling members remain active and accept MPLS IP traffic. Also, the link-bundle interface accepts the **mpls ip** command if you enter this command while a member is coming up and is being added to the link-bundle interface.

Conditions: These symptoms are observed on a Cisco 12000 series running Cisco IOS Release 12.0(28)S when an MTU value higher than 9180 is configured on the link-bundle interface.

Workaround: Remove the MTU configuration from the link-bundle interface.

- CSCee22450

Symptoms: A subinterface on a Cisco 10000 series may drop packets because of unicast RPF check failures, even though the interface is not configured with uRPF.

Conditions: This symptom is observed on an ATM interface with several subinterfaces when there is at least one subinterface that has uRPF configured. Disabling uRPF on the subinterface still leaves uRPF enabled, even though the CLI indicates it is not enabled. This may also occur with Frame Relay subinterfaces.

Workaround: Select a subinterface that has uRPF configured, then deconfigure and reconfigure it. This updates all subinterfaces on the interface in such a way that uRPF is correctly enabled or disabled.

- CSCee22810

Symptoms: On a Cisco 7500 series, all PVCs may suddenly enter the down state and remain in this state for about two minutes before they come back up. During the DLCI down state, the subinterface does not go down and no notifications are observed in the message log.

Conditions: This symptom is observed on a Cisco 7500 series that is configured with an RPS4+ or an RSP8 and that runs the rsp-jsv-mz image of Cisco IOS Release 12.2(12i). In addition, the router is configured with an 8-port serial port adapter and an HSSI port adapter, is configured for Frame Relay, and has more than 450 PVCs/DLCIs. Note that the symptom may be platform-independent and may also occur on other Cisco platforms in a similar configuration.

Workaround: There is no workaround.

- CSCee22933

Symptoms: CBR-type or VBR-type VP cell-relay or cell-packing AToM VCs may not be able to retain their bandwidth to the configured CBR or VBR shaping rate. This situation persists even when the total shaping rate of the VPs and VCs is far below the physical bandwidth of the interface.

Conditions: This symptom is observed when there are many other cell-relay or cell-packing AToM VCs configured.

Workaround: There is no workaround.

- CSCee24263

Symptoms: A PVC may be inactive and may not come up.

Conditions: This symptom is observed when a VC is deleted or removed and you try to recreate the same VC.

Workaround: Save the configuration and reload the router.

- CSCee25588

Symptoms: A 12000 series Engine 2 line card may not accept a “tx-cos” configuration.

Conditions: This symptom is observed if the router previously had an Engine 4+ line card in the same slot and this Engine 4+ line card was configured with an output service policy.

Workaround: Reload the router.

- CSCee28481

Symptoms: After working fine for sometime, a 4-port OC-12 ATM line card stops forwarding unicast packets to the RP, and none of the unicast traffic that is sourced from or destined to the RP via the 4-port OC-12 ATM line card goes through. Unicast traffic to the 4-port OC-12 ATM line card interfaces fails too.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(21)ST7 when MPLS is enabled on the line card. IP traffic and IS-IS traffic that pass through the router are not affected. To recover the line card, reset the line card.

Workaround: There is no workaround.

- CSCee28754

Symptoms: GE interfaces on an EPA-GE/FE-BBRD line card may drop tag packets.

Conditions: The problem is reported on a Cisco 12000 series running Cisco IOS Release 12.0(23)S5 only when you perform an OIR of an EPA-GE/FE-BBRD to install or remove additional EPA-3GE-SX/LH line cards.

Workaround: Perform a second OIR of the line card.

- CSCee29196

Symptoms: When a Cisco 10000 series does not have a specific route for both end points of a voice connection, the Cisco 10000 series duplicates one-way audio only for the specific route that populates its routing table, not for the end point that uses the default route from the routing table.

Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.0(25)S3 and that is configured with a PRE-1.

Workaround: There is no workaround.

- CSCee30089

Symptoms: If a multilink interface loses members of the bundle, or if you enter the **shutdown** command followed by the **no shutdown** command on a multilink interface, or if the router reloads, the bandwidth that is allocated for non-real time classes can be allocated incorrectly. The sum of the bandwidth that is allocated for non-real time classes and the bandwidth that is specified by the **police bps** command for real time traffic may exceed the actual bandwidth of a multilink interface.

Conditions: This symptom is observed on a Cisco 10000 series running Cisco IOS Release 12.0(27)S1 that has the **service-policy out** command enabled on a multilink interface. The service policy consists of a real-time class and several classes with reserved bandwidth. The real-time class is configured with the **priority** command and the **police bps** command. Other classes are configured with the **bandwidth bandwidth-kbps** command.

The bandwidth that is allocated for non-priority traffic should take into account the bandwidth that is reserved by the **police bps** command for the real-time class.

Workaround: Remove and reapply the **service-policy out** command to the multilink interface.

- CSCee30527

Symptoms: After reloading a Cisco 12000 series, the following message may be seen on an Engine 2 or Engine 3 line card:

```
%MBUS-2-DNLDFAIL: IOS download to slot 7 fail, timeout
```

In some cases this situation may prevent the line card from coming up:

```
%GRP-3-ABANDON_DOWNLOAD: End attempt to start the linecard in slot 7
```

Conditions: This symptom is observed rarely on a Cisco 12000 series that is running the gsr-p-mz image of Cisco IOS Release 12.0(28)S.

Workaround: The line card may come up when you reload the router again.

- CSCee30549

Symptoms: Some interfaces on a channelized SONET line card may not carry bidirectional traffic following an APS switchover. Interfaces may be up and routes may be present when this occurs.

Conditions: The symptom is only observed on a Cisco 12000 series 1-port OC-12 line card (channelized to DS1) that functions in an 1+1 APS configuration. The symptom could occur on any channelized APS interface.

Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the affected interfaces.

- CSCee30966

Symptoms: A 1-port OC-12 Channelized to DS1/E1 ISE line card may fail to come up when you boot the router or reload the line card.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S.

Workaround: There is no workaround.

- CSCee31105

Symptoms: A wrong aggregate NetFlow cache prefix may occur when an extended Deny ACL is configured with AGNF. You are supposed to find one prefix entry in the cache but there are two prefix entries.

Conditions: This symptom is observed when an extended Deny ACL is configured with AGNF on a Cisco 12000 series Engine 3 16-port OC-3 POS line card.

Workaround: There is no workaround.

- CSCee31196

Symptoms: An LDP session over a tunnel interface may drop and not come back up.

Conditions: This symptom is observed on a Cisco router running Cisco IOS Release 12.0(27)S1 when auto-tunnel traffic engineering is configured and when RSVP label distribution is configured in the MPLS core.

Workaround: Run LDP in the MPLS core for all interfaces that have auto-tunnel traffic engineering configured.

- CSCee32208

Symptoms: After a circuit bounces, traffic stops being passed on a VC when using a VC bundle. Other VCs on the same subinterface still work. The switch on the other side of the VC does not show any received cells from the VC.

In addition, the **show atm vc** command does not work because even after the VC is recovered, the command output still does not show any traffic.

Conditions: These symptoms are observed on a Cisco 12000 series.

Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the affected subinterface.

- CSCee32365

Symptoms: When a single bundle link associated with a Multilink Frame Relay (MFR) interface is brought up, LMI exchanges over the MFR interfaces may not happen.

Conditions: This symptom is observed on a Cisco 7500 series that is configured for MFR.

Workaround: There is no workaround.

- CSCee32484

Symptoms: After performing a manual switchover on a dual-RP router that functions in RPR+ or SSO mode, the following error message may be seen on an 8xOC3ATM line card, and the line card may stop forwarding traffic:

```
%QM-4-STUCK: Port 0 Queue mask 0x80
```

Conditions: This symptom is observed on a Cisco 12000 series that is running the gsr-p-mz image of Cisco IOS Release 12.0(28)S.

Workaround: Perform a microcode reload on the line card.

- CSCee32921

Symptoms: Line cards in a Cisco 12000 series dual-RP router running Cisco IOS Release 12.0(28)S may fail when the active RP is reloaded.

Conditions: This symptom is observed when the active RP is reloaded by entering the **microcode reload** command.

Workaround: There is no workaround.

- CSCee34133

Symptoms: If CEF fails, you cannot enable CEF IPv6 by entering the **ipv6 cef distributed** command.

Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of Cisco IOS Release 12.0(28)S.

Workaround: There is no workaround.

- CSCee34469

Symptoms: The feature manager queue and the Qos manager queue on the Route Processor (RP) may not drain for 20 minutes after a reload in a scaled environment with 1400 IP and L3VPN connections (subinterfaces). The feature manager pushes ACL and PBR configurations to the IP Services Engine (ISE) line cards for TCAM processing. The QoS manager pushes CAR/MQC configurations to the ISE line cards for TCAM processing.

You can monitor the state of the feature manager queue with the **show fm queue** command. You can monitor the state of the QoS manager queue with the **show qm queue** command.

Conditions: This symptom is observed on a 12000 series running Cisco IOS Release 12.0(28)S. The symptom occurs with SSO/NSF two times out of five tests but has not been observed with RPR.

Workaround: There is no workaround.

- CSCee34474

Symptoms: Open Shortest Path First (OSPF) peers are mapped to the wrong subinterfaces.

Conditions: This symptom is observed on a Cisco 10000 series after a high availability (HA) switch has occurred over ATM interfaces and OSPF adjacencies have been formed.

Workaround: There is no workaround.

- CSCee34622

Symptoms: Neighbor adjacencies for the IS-IS, OSPF, or other routing protocol may bounce during a Nonstop Forwarding (NSF) switchover.

Conditions: This symptom is observed when you enable a routing protocol for NSF and you enter the **external overload signalling** router configuration command. The following configuration illustrates this situation for IS-IS:

```
router isis area-tag
nsf [cisco | ietf]
external overload signalling
```

Workaround: Disable the **external overload signalling** router configuration command.

- CSCee35659

Symptoms: A priority class cannot be configured if the remaining bandwidth is used on the existing classes. Such a service policy is rejected.

Conditions: This symptom is observed on Cisco 12000 series-ISE based line cards.

Workaround: Use police actions in the priority class in conjunction with bandwidth percentages on the existing classes.

- CSCee36744

Symptoms: An RP may crash when you add or remove a channel group to or from a 4-port ISE Gigabit Ethernet line card or when you reload microcode onto the line card on which channel group members are configured.

Conditions: This symptom observed on a Cisco 12000 series when there are link-bundle subinterfaces configured on the 4-port ISE Gigabit Ethernet line card. A list of the affected releases can be found at <http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCed63480>. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

Workaround: There is no workaround.

- CSCee37430

Symptoms: MPLS-to-IP traffic may not recover after a manual RP switchover in SSO mode.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(29)S and occurs only for prefixes that have static routes configured.

Workaround: Enter the **clear ip route network** EXEC command in which the *network* argument is the network or subnet address for which forwarding no longer functions after the manual RP switchover.

- CSCee39733

Symptoms: VLAN packets with SNAP headers are switched into an xconnect link.

Conditions: This symptom is observed when you send traffic from one CE router via a PE router to another CE router. The expected behavior is that the VLAN packets with SNAP headers are dropped at the PE router but instead they are forwarded to the other CE router.

Workaround: There is no workaround. However, VLAN functionality is not impacted.

- CSCee39854

Symptoms: A ping or Telnet connection to a connected CE router may fail from a Cisco 12000 series router that functions as a PE router.

Conditions: This symptom is observed on Cisco 12012 that runs Cisco IOS Release 12.0(21)ST3 or a later release when the router has a 3-port Gigabit Ethernet line card that is configured for dot1q encapsulation on its subinterfaces.

This symptom occurs because of a misconfiguration on the subinterfaces: when you configure a subinterface with new a VRF without removing the already configured VRF, the symptom occurs.

Workaround: Unconfigure and reconfigure the VRF configuration on the misconfigured subinterfaces.

- CSCee40349

Symptoms: Cisco 12816 and 12810 routers need to have specific MBSU 5v and on-board 5v thresholds other than the values in the legacy system. Otherwise, there may be error messages in the console logs that complain that the voltages are abnormal.

Conditions: This symptom is observed on Cisco 128xx series routers.

Workaround: The **no show environment** command can be configured, but only if this problem is seen.

- CSCee40938

Symptoms: FRoMPLS traffic fails with an Engine 3 line card as the disposition card.

Conditions: This symptom is observed with any DLCI (xx xxxx xx11) that uses the two LSBs in its “ckt” ID. This problem is seen because of the corruption of the two LSBs during a disposition update.

Workaround: There is no workaround.

- CSCee41413

Symptoms: An active PRE on a Cisco 10000 series may crash.

Conditions: This symptom is observed when the standby PRE goes down just when the driver of a CHSTM1 or CHOC12 line card attempts to synchronize a linestate message.

Workaround: Avoid resetting the standby PRE unnecessarily.

- CSCee41728

Symptoms: Some voltage threshold levels may not be set correctly and may cause a line card to power down without any warning messages if the voltage drops below 3v.



Note Note: There has been no reports of this happening yet.

Conditions: This symptom is observed on Cisco 12000 series routers.

Workaround: The **no show environment** command can be configured, but only if this problem is seen.

- CSCee42198

Symptoms: Engine 4+ loadsharing does not work correctly in a VPN imposition situation. The problem is not seen with Engines 0, 2 and 3.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(27)S when traffic enters on a VRF interface and is loadshared over four links to the core. Traffic is loadshared over only two of the four links.

Workaround: Use three-path loadbalancing.

- CSCee42279

Symptoms: During an L2TPv3 test with a Cisco 12000 series 4-port OC-12 ATM line card, when you bump traffic on more than two ports that process a high rate of traffic, traffic may stop. When this situation occurs, the CPK24 FPGA on the line card generates ingress packet length errors and sometimes SDRAM CRC errors.

Conditions: This symptom is observed on a 4-port OC-12 ATM line card that is configured for L2TPv3 and that is installed in a Cisco 12000 series that runs the gsr-p-mz image of Cisco IOS Release 12.0 S.

Workaround: Reload the line card.

- CSCee42281

Symptoms: Some interfaces on a channelized SONET line card may not carry bidirectional traffic following an APS switchover. Interfaces may be up and routes may be present when this occurs.

Conditions: The symptom is observed on Cisco 12000 series Engine 3 channelized line cards (OC-48 or 4XOC-12 channelized to DS-3) that functions in an 1+1 APS configuration. However the symptom could occur on any channelized APS interface.

Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the affected interfaces.

- CSCee43562

Symptoms: The feature manager queue on the Route Processor may not drain for 20 minutes after a reload in a scaled environment with 1400 IP and L3VPN connections (subinterfaces). The feature manager pushes ACL and PBR configurations to the IP Services Engine (ISE) line cards for TCAM processing. You can monitor the state of the feature manager queue with the **show fm queue** command.

Conditions: This symptom is observed on a 12000 series that runs Cisco IOS Release 12.0(28)S and may occur on any ISE line card that uses an associate message in the QoS manager.

Workaround: There is no workaround.

- CSCee43880

Symptoms: After reloading an E2 16-port OC-3 POS line card that is a member line card of POS channel, the peer POS channel members do not become active members again.

Conditions: The symptom is observed on a link-bundling interface of a Cisco 12000 series router that runs Cisco IOS Release 12.0 S.

Workaround: There is no workaround.

- CSCee45099

Symptoms: A Cisco 12000 series 8-port OC-48 or 2-port OC-192 line card may crash.

Conditions: This symptom is observed when the line card is configured for MPLS-TE FRR.

Workaround: There is no workaround.

- CSCee49862

Symptoms: A Cisco 7500 series multichannel T3 port adaptor (PA-MC-2T3+) may not provide a two-second delay before bringing down the T3 controller.

Conditions: This symptom is observed when an alarm as defined in the ANSI T1.231 specification occurs.

Workaround: There is no workaround.

- CSCee49983

Symptoms: When the controller of multichannel T3 port adaptor (PA-MC-2T3+) goes down for a short duration and an alarm occurs, the port adaptor does not report the type of alarm.

Conditions: This symptom is observed on a Cisco 7200 series and Cisco 7500 series that are configured with a PA-MC-2T3+. The port adaptor should provide a history table of recent alarm conditions along with a corresponding time stamp to allow for proper troubleshooting.

Workaround: There is no workaround.

- CSCee51126

Symptoms: A Cisco 12000 series may drop 2 to 3 percent of the ping packets that are destined to the router when the input interface is an Engine 4+ line card.

Conditions: This symptom is observed for ICMP packets on a Cisco 12000 series that is Cisco IOS Release 12.0(26)S1. The symptom may also affect other types of packets.

Workaround: There is no workaround.

- CSCee51909

Symptoms: An Engine 3 channelized (OC-48 to DS3) line card that processes traffic crashes.

Conditions: This symptom is observed when you change the MTU on the E4+ disposition line card.

Workaround: There is no workaround.

- CSCee53458

Symptoms: After you boot a Cisco 12000 series, one of the members of a link bundle that has eight members that are configured on an Engine 2 16-port O-C3 POS line card shows up in both the active and passive lists.

Conditions: This symptom is observed on a Cisco 12000 series that runs an interim release of Cisco IOS Release 12.0(28)S.

Workaround: There is no workaround.

Further Problem Description: Proper functionality is not impacted by this caveat.

- CSCee53461

Symptoms: BGP adjacencies may time out on an Engine 3 channelized OC-12 line card.

Conditions: This symptom is observed on a Cisco 12000 series when you use Multilink PPP (MLP) interfaces with service policies attached.

Workaround: There is no workaround.

- CSCee53472

Symptoms: Interfaces of a line card may stay in the link down and line down states when you create an initial configuration on a new line card.

Conditions: This symptom is observed on a Cisco 10000 series when a previously unprovisioned line card is introduced into the system and a new configuration is entered for this line card.

Workaround: After inserting the new line card, save the configuration and reboot the router.

- CSCee53667

Symptoms: A ping to an interface of an Engine 3 Gigabit Ethernet line card fails after an RP switchover occurs.

Conditions: This symptom is observed on a Cisco 12000 series that functions in SSO HA mode when an RP switchover occurs after the line card has been reloaded.

Workaround: There is no workaround.

- CSCee54143

Symptoms: An E1 port on a PA-MC-8T1 port adapter may stay down after a VIP crash.

Conditions: This symptom is observed on a Cisco 7513 that is configured with a VIP in which a PA-MC-8T1 port adapter with a channelized E1 (or T1) port is installed in slot 0.

Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the affected interface.

- CSCee54198

Symptoms: A Cisco 12000 series crashes because of a bus error.

Conditions: This symptom is observed on a Cisco 12016 that runs Cisco IOS Software 12.0(25)S2 when you enter the **hw-module slot 17 shutdown** command to shut down the master scheduler card.

Workaround: Do not shut down the master scheduler card.

- CSCee55297

Symptoms: When you suspend and resume the event manager scheduler and an applet tries to register, the registration fails with an error from the operating system.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0 S or Release 12.2 S. However, the symptom may also occur in other releases.

Workaround: There is no workaround.

- CSCee55416

Symptoms: On a Cisco 12000 series that is configured with dual RPs, the primary RP may fail to ping itself when you reload a 4-port Gigabit Ethernet ISE line card and then you shut down the CSC1. Doing so causes the active RP to force a crash, causing a switchover to the secondary RP.

Conditions: This symptom observed on a Cisco 12000 series that runs an interim release of Cisco IOS Release 12.0(29)S.

Workaround: There is no workaround.

- CSCee55457

Symptoms: When a channel group (for example, channel +1) is removed from a controller, the class-default queue gets stuck on the next time slot/channel.

Conditions: This symptom is observed on a Cisco 10000 series that is configured with 24-port channelized E1/T1 line cards and that has a high traffic rate on the removed channel.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command.

- CSCee56199

Symptoms: An egress IPv6 QoS policy does not work after a Cisco 12000 series reboots.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0 S when the following conditions are met:

- An IPv6 ACL is used to match traffic.
- UDP ACEs are used in the IPv6 ACL.
- Matching UDP traffic is sent.

Note that matching TCP traffic works fine.

Workaround: There is no workaround.

- CSCee56347

Symptoms: A service policy that has the **police cir percent** command enabled does not take effect on an interface.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0 S.

Workaround: Enter the **police cir percent** command and use an absolute value instead of a percentage.

- CSCee57310

Symptoms: When you remove one link from an MLP bundle that has eight links and that is passing bidirectional traffic, the traffic may not recover on one end.

Conditions: This symptom is observed on a Cisco 12000 series Engine 3 channelized OC-12 line card and occurs only when bidirectional traffic is being passed.

Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the MLP interface.

- CSCee57438

Symptoms: The second port pair (interface SRP x/1) of an Engine 4+ 4-port OC-48 DPT line card is unable to forward traffic (including pings) at layer 3. The first port is also damaged (interface SRP x/0); a portion of its forwarding capabilities is damaged. The layer 2 SRP protocol operates correctly.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(27)S1 and does not require any specific trigger: the symptom is always there.

Workaround: There is no workaround.

- CSCee57485

Symptoms: There are two symptoms:

- Packets with explicit null labels may be dropped from an Engine 4+ POS line card.
- CEF may become disabled on an Engine 4+ POS line card.

Conditions: These symptoms are observed on a Cisco 12000 series under the following conditions:

- The router functions as a PE router with the Engine 4+ POS line card facing the core and performing MPLS disposition.
- VRFs are configured on the router.
- The Explicit Null feature is enabled on the router.

Workaround: There is no workaround.

- CSCee58770

Symptoms: A Cisco router may generate the following error message:

```
%TUN-5-RECURDOWN: Tunnel2 temporarily disabled due to recursive routing
```

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(26)S2 and that is configured with a tunnel services card (TSC) (that is, a 1-port OC-48 POS line card) when MPLS TE tunnels are configured on the router and when static routes are added.

Workaround: There is no workaround.

- CSCee59106

Symptoms: The performance of an OC-48 to E3 concatenated or channelized line card may drop from 4 Mpps to 2.84 Mpps when oCAR is enabled in a configuration that includes both the **conform-action** and **exceed-action** keywords and when oCAR is transmitting packets and changing the precedence.

Conditions: This symptom is observed on a Cisco 12000 series that runs the c12kprp-p-mz image of Cisco IOS Release 12.0(28)S or an earlier release. However, note that performance drops do not occur in Release 12.0(27)S1.

Workaround: There is no workaround.

- CSCee63939

Symptoms: An Engine 6 line card may crash during the MDFS process.

Conditions: This symptom is observed on a Cisco 12000 series when multicast and unicast traffic are running through the Engine 6 line card.

Workaround: There is no workaround.

- CSCee65004

Symptoms: A 1-port 10-Gigabit Ethernet line card (1X10GE-LR-SC) may crash, reporting %TX192-3-CPUIF errors.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(27)S1 when you shut down the 10GE port of a 4-port 10 Gigabit Ethernet module (WS-X6704-10GE) that is installed in a Cisco 7609 at the other side of the connection.

Workaround: There is no workaround.

- CSCee67207

Symptoms: A public recursive route is not labeled.

Conditions: This symptom is observed on a Cisco router that functions as a BGP peer and that has the **neighbor name send-label** command enabled as part of an IPv4 address family, which is required for Inter-AS configurations. The symptom affects routers that perform MPLS forwarding using ASICs such as some Cisco 7200 series routers, the Cisco 7304, the Cisco 10000 series, the Cisco 12000 series, and the Cisco RPM-XF. (This list may not be exhaustive.)

Workaround: There is no workaround. Note that the symptom does not occur if the **neighbor name send-label** command is enabled as part of an IPv4 address family VRF.

- CSCee67746

Symptoms: An E4+ POS line card reports %TX192-3-PAM_MODULE and %TX192-3-PAM_PIM errors. On rare occasions the line card may crash when it receives a malformed packet.

Conditions: These symptoms are observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(25)S3 or Release 12.0(26)S4.

Workaround: There is no workaround.

- CSCee68666

Symptoms: It may take up to 1 second for a line card to notify the RP about a physical layer failure alarm. This situation prevents fast sub-second IGP convergence.

Conditions: This symptom is observed in a non-FRR and non-APS configuration.

Workaround: There is no workaround.

- CSCee70478

Symptoms: If hardware multicast forwarding is enabled on an Engine 2 line card that is connected to the source of multicast traffic, multicast traffic may not be forwarded after the router has reloaded.

Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of Cisco IOS Release 12.0(27)S2.

Workaround: Remove and reapply hardware multicast forwarding to the line card.

- CSCee70591

Symptoms: A Cisco 7500 series T3 port adapter (PA-2T3+) may not provide a two-second delay before bringing down the T3 controller.

Conditions: This symptom is observed when an alarm as defined in the ANSI T1.231 specification occurs.

Workaround: There is no workaround.

- CSCee71156

Symptoms: Unexpected behavior may occur when the **tx-ring-limit** *ring-limit* command and HQF are configured: a memory leak may occur in the pool manager of the router.

Conditions: This symptom is observed when traffic is sent at high speed (higher than the line rate) and when the *ring-limit* argument is less than 255.

Workaround: There is no workaround.

- CSCee72027

Symptoms: WRED does not share WRED labels even when WRED parameters are identical. Because Engine 4 and Engine 4+ line cards have only seven WRED labels, when you configure WRED for all eight IP precedences, the line cards display the following error:

```
% Can not configured WRED, all WRED labels are in use.
```

This situation prevents part of the **precedence** (WRED group) command for the 8th IP precedence from being applied to the interface policy map.

Conditions: This symptom is observed when you apply a policy map that uses more than seven WRED labels and when WRED labels are not shared.

Workaround: There is no workaround.

- CSCee72353

Symptoms: An LDP session over a tunnel interface may drop and not come back up.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0 S when auto-tunnel traffic engineering is configured and when RSVP label distribution and LDP are configured in the MPLS core.

If the **no mpls ip** command is configured on the physical interface to disable LDP, and RSVP label distribution remains enabled, auto-tunnel traffic engineering fails and you cannot bring the tunnel back up.

Workaround: Run LDP in the MPLS core for all interfaces that have auto-tunnel traffic engineering configured.

- CSCee73182

Symptoms: A channel-group link-bundling configuration may disappear from a member interfaces configuration when you reload the router.

Conditions: The symptom is observed on a link-bundling interface (for both POS and GE) on a Cisco 12000 series that runs a Cisco IOS interim release of Release 12.0(29)S.

Workaround: Configure the channel group on the link-bundle member interfaces after the router has reloaded.

- CSCee73410

Symptoms: When you enter the **redundancy force-switchover** command, IPC messages and tracebacks may be generated on an Engine 2 3-port GE line card.

Conditions: The symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S or an earlier release and that has dual GRPs or dual PRPs.

Workaround: There is no workaround.

- CSCee74256

Symptoms: When SSO is configured and the Event Manager triggers a switchover, the new active RP reloads unexpectedly.

Conditions: This symptom is observed on a Cisco 12000 series.

Workaround: There is no workaround.

- CSCee74419

Symptoms: When L3 VPN routes flap, the PLU utilization on line cards in a PE router may increase to and remain at 99 percent.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S and that functions as a PE router when L3 VPN routes flap in an L3 VPN network that has a large number of VPN routes.

Workaround: There is no workaround.

- CSCee74886

Symptoms: After you enter the **microcode reload pxf** command or after a PXF crash occurs, EoMPLS packets that should be encapsulated with EoMPLS encapsulation are treated as if they are normal IP packets, and are likely to be dropped by the router.

Conditions: This symptom is observed on a Cisco 10720 router when an SRP (sub)interface is used as the EoMPLS backbone interface to transport EoMPLS packets to other EoMPLS PE routers and when the (sub)interface has the **xconnect destination-address vc-id encapsulation mpls** command enabled.

Workaround: Remove the **xconnect destination-address vc-id encapsulation mpls** command from the (sub)interface that connects to a customer device, and reconfigure it on the (sub)interface.

- CSCee75225

Symptoms: High CPU utilization may cause interfaces to flap, and the following spurious memory access messages may be generated:

```
%ALIGN-3-SPURIOUS: Spurious memory access made at 0x603C2724 reading 0x194
%ALIGN-3-TRACE: -Traceback= 603C2724 601D2888 601D40B4 00000000 00000000 00000000
00000000 00000000
```

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(23)S when you the **clear cef linecard** command.

Workaround: There is no workaround.

- CSCee75296

Symptoms: The MTU range for a link bundle on an 8-port OC-3 Engine 2 POS line card starts at zero.

Conditions: This symptom is observed on a Cisco 12000 series that runs a Cisco IOS interim release of Release 12.0(29)S.

Workaround: There is no workaround.

- CSCee76476

Symptoms: A Cisco 12000 series equipped with Engine 4 or Engine 6 line cards may crash because of an unexpected exception to CPU vector 300 when the CISCO-CLASS-BASED-QOS-MIB is queried via SNMP.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(26)S or an earlier 12.0 S release.

Workaround: There is no workaround other than excluding the access to the MIB.

- CSCee77227

Symptoms: When a channel group is removed and readdded to the controller, and then a PRE switchover occurs, the PPP line protocol on the readdded channel goes down after a while.

Conditions: This symptom is observed on a Cisco 10000 series that is configured with 24-port channelized E1/T1 line cards.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface.

- CSCee77744

Symptoms: An ISE line card that is configured for IPv6 and that has traffic flowing through it may reload when you enter the **no ipv6 unicast-routing** command.

Conditions: This symptom is observed on a Cisco 12000 series only when you enter the **no ipv6 unicast-routing** command.

Workaround: Stop the IPv6 traffic before you enter the command.

- CSCee77867

Symptoms: A standby PRP that functions in SSO mode continues to reset.

Conditions: This symptom is observed on a Cisco 12406 that runs a Cisco IOS interim release for Release 12.0(29)S and that is has an ATM VC bundle configuration.

Workaround: Reload the standby PRP without the ATM VC bundle and re-apply the ATM VC bundle after the standby PRP has booted.

- CSCee78118

Symptoms: A line card or port adapter may crash on an MPLS VPN PE router when the customer-facing interfaces are flapped.

Conditions: This symptom is observed when any of the following conditions are present:

- eBGP is used as the routing protocol between the PE and CE router, the CE router has the **redistribute connected** command enabled in the BGP configuration, and there are multiple eBGP sessions between the PE and CE router.
- The connected route for the link between the CE and PE router is learned from another PE router via MP-iBGP. For example, the CE router may be dual-homed and may advertise the connected routes to both PE routers.

The symptom affects routers that perform MPLS forwarding using ASICs such as some Cisco 7200 series routers, the Cisco 7304, the Cisco 10000 series, the Cisco 12000 series, and the Cisco RPM-XF. (This list may not be exhaustive.)

Workaround: Avoid the above-mentioned conditions. For example, avoid the **redistribute connected** command in the BGP configuration of the CE router.

- CSCee78567

Symptoms: A temporary counter condition in which you see very large MPLS TE tunnel counter spikes may occur on a Cisco 12000 series. This situation is observed via the SNMP variable IfHCOutOctets (the total number of octets transmitted), via the SNMP variable locIfOutBitsSec (the Cisco 5-minute decaying average), and in the output of the **show interfaces tunnel number** privileged EXEC command (observe the elevated output rate).

Conditions: This temporary counter condition is observed only for one or two sample periods and affects the MPLS-TE auto-bandwidth mechanism because the collection timer may be invoked at a time while the counter is at an extreme value. If the auto-bandwidth mechanism collection value is greater than the physical interface capability, the LSP tunnel build fails at the next LSP tunnel build.

Workaround: There is no workaround.

- CSCee79125

Symptoms: The standby RP may notify client applications about a state-change event even if there is no change in the state.

Conditions: This symptom is observed on a Cisco 10008 that runs Cisco IOS Release 12.0S. However, the symptom is platform-independent.

Workaround: There is no workaround.

- CSCee80041

Symptoms: A line card with an ATM QoS configuration may crash.

Conditions: This symptom is observed on a Cisco 12406 that runs a Cisco IOS interim release of Release 12.0(29)S.

Workaround: There is no workaround.

- CSCee80214

Symptoms: When you delete shaping by entering the **no shape** *cir* command, shaping seems to be disabled on all interfaces, which can be seen in the output of the **show policy-map interface** *interface-name* command. However, the output of the **show policy-map** *policy-map* command still shows the shape value.

Conditions: This symptom is observed on Frame Relay subinterfaces on a Cisco 10000 series.

Workaround: Remove and reconfigure the Frame Relay class on each subinterface or remove the policy map from the map class and reconfigure the policy map.

- CSCee80281

Symptoms: When a policy-map class configuration command that configures a queue (for example, the **bandwidth** *kbps* command) is enabled on a Fast Ethernet interface and when the speed of this interface changes, the router crashes.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(29)S.

Workaround: There is no workaround.

- CSCee81490

Symptoms: MALLOCFAIL messages may be generated during an attempt to allocate large negative and positive memory blocks in the “cpf_process_ipcQ” process:

```
%SYS-2-MALLOCFAIL: Memory allocation of -1622998781 bytes failed from 0x60B5BE48,
alignment 0
Pool: Processor Free: 371055532 Cause: Not enough free memory
Alternate Pool: None Free: 0 Cause: No Alternate pool
-Process= "cpf_process_ipcQ", ipl= 0, pid= 141
-Traceback= 603DDCB0 603E005C 60B5BE50 60B5C140 60B5C62C 60B59A0C 603D5D1C 603D5D08

%SYS-2-MALLOCFAIL: Memory allocation of 344820739 bytes failed from 0x60B5BE48,
alignment 0
Pool: Processor Free: 363937412 Cause: Memory fragmentation
Alternate Pool: None Free: 0 Cause: No Alternate pool
-Process= "cpf_process_ipcQ", ipl= 0, pid= 141
-Traceback= 603DDCB0 603E005C 60B5BE50 60B5C140 60B5C62C 60B59A0C 603D5D1C 603D5D08
```

Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.0(24)S5.

Workaround: There is no workaround.

- CSCee81787
Symptoms: A VIP crashes with a “DRQ stalled” error message.
Conditions: This symptom is observed when a switchover occurs on a Cisco 7500 series.
Workaround: There is no workaround.
- CSCee82088
Symptoms: The output of the **show controller au-4-tug-3** command does not show any detailed TUG groups under the controller.
Conditions: This symptom is observed on the Cisco 10000 series that is configured with a channelized STM-1 line card.
Workaround: Enter the following sequence of commands on the router to restore the display of the **show controller au-4-tug-3** command:

```
router# config terminal
router(config)# hw-module slot <slot number> shutdown
router(config)# no hw-module slot <slot number> shutdown
router(config)# end
```
- CSCee82681
Symptoms: On an RTR probe, an RSP does not report input or output packets for serial interfaces of PA-MC-8T1, PA-MC-8E1, and PA-MC-8TE1+ port adapters.
Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.2(23a) or Release 12.3 and is more likely to occur when the number of channelized port adapters (such as the PA-MC-8T1, PA-MC-8E1, and PA-MC-8TE1+ port adapters) that are installed in the router is high. The symptom may also occur in other releases.
Workaround: Reload the router.
Alternate Workaround: Enter the **reload microcode** router configuration command.
- CSCee83781
Symptoms: A Cisco router may reload when you enter the **show ipv6 mfib verbose** command for a large MFIB.
Conditions: This symptom is observed on a Cisco 12000 series that is configured for multicast.
Workaround: There is no workaround.
- CSCee84496
Symptoms: An NPE-G1 may display an erroneous parity error message.
Conditions: This symptom is observed on a Cisco 7200 series when the NPE-G1 receives an ECC/bus error.
Workaround: There is no workaround.
- CSCee84732
Symptoms: The CPU utilization of a router that is configured for Multiprotocol Label Switching (MPLS) may temporarily increase to 80 or 90 percent when a peer router is reloaded or when an interface with a large number of numbered subinterfaces is administratively enabled.
Conditions: The symptom is observed in a rare situation when label distribution protocol (LDP) is used in configurations with a very large number of numbered interfaces. When this problem occurs, the output of the **show process cpu sorted** command shows that the “Tagcon Addr” process consumes the majority of the CPU cycles.
Workaround: There is no workaround.

- CSCee84933

Symptoms: A 1-port 10-Gigabit Ethernet line card (1X10GE-LR-SC) may crash, reporting a stack trace pointing to the optics interrupt handler.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(27)S1 when you shut down the 10GE port of a 4-port 10 Gigabit Ethernet module (WS-X6704-10GE) that is installed in a Cisco 7609 at the other side of the connection.

Workaround: There is no workaround.
- CSCee88296

Symptoms: A Cisco 12000 series reloads unexpectedly when you configure an MPLS TE tunnel.

Conditions: This symptom is observed when a PVC bundle is configured on an interface or subinterface and when you configure an MPLS TE tunnel on the same interface or subinterface.

Workaround: There is no workaround.
- CSCee88364

Symptoms: A **set** command may not have any effect on traffic and packets are not marked.

Conditions: This symptom is observed when a **set** command is enabled in a policy map that is attached to an interface.

Workaround: There is no workaround.
- CSCee90155

Symptoms: A TLU memory leak occurs on an Engine 3 line card that has aggregate IPv6 labels when the associated IPv6 route is flapped or changed.

Conditions: This symptom is observed when you inject static routes that point out of a Gigabit Ethernet (GE) interface of a 4-port GE ISE line card and when the GE interface is flapped.

Depending on the number of aggregate IPv6 labels, the TLU memory leak can be either service-impacting or very minor.

Workaround: There is no workaround.
- CSCee90295

Symptoms: A Cisco 12000 series may reload when you configure a large number of class maps.

Conditions: This symptom is observed on a Cisco 12816 that has a PRP and that runs Cisco IOS Release 12.0(28)S.

Workaround: Configure a maximum of 255 classes per parent policy map.
- CSCee90552

Symptoms: When you send an SNMP query to poll the CBQOS MIB, high CPU utilization may occur. Depending on number of service policies attached, the CPU utilization may reach 100 percent, causing many different negative effects to occur: the Telnet connection may go down, LDP may go down, and in some cases the router may crash.

Conditions: This symptom most likely occurs when the unsupported cbQosREDClassStats objects are polled and when there are about 1000 QoS policy attachment configured.

Workaround: The potential workarounds include the following:

 - Reduce the number of QoS policy attachments.
 - Avoid polling the unsupported stats table(s).
 - Reduce the polling frequency.

- CSCee90590

Symptoms: A 6-port OC-3 POS line card (ESR-6OC-3/P-SMI=) may go down unexpectedly, and the following error messages may be logged (assuming that the line card is installed in slot 6 of the router):

```
IPCOIR-4-REPEATMSG: IPC handle already exists for 6/0
IPCOIR-2-CARD_UP_DOWN: Card in slot 6/0 is down. Notifying 6oc3pos-1 driver.
C10K_ALARM-6-INFO: ASSERT CRITICAL slot 6 Card Stopped Responding OIR Alarm -
subslot 0
```

Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.0(27)S2 in a dual-PRE configuration when the CPU utilization on the active PRE is high. The symptom may also occur in other 12.0 S releases.

Workaround: There is no workaround.

- CSCee90893

Symptoms: An RP may crash if a policy map matches a QoS group value that is greater than seven.

Conditions: This symptom is observed on an interface of a Cisco 12000 series Engine 4+ line card when the interface is configured for shaping.

Workaround: Use a QoS group value in the range of one through seven in the policy map.

- CSCee91240

Symptoms: PRP crashes after you remove a port-channel interface.

Conditions: This symptom is observed on a Cisco 12000 series running that runs a Cisco IOS interim release for Release 12.0(30)S.

Workaround: There is no workaround.

- CSCee93228

Symptoms: Under certain unknown circumstances, a traceroute may trigger a process watchdog.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(26)S2. However, the problem is not specific to a Cisco 12000 series or to Cisco IOS Release 12.0S and may occur on other platforms and in Release 12.2T and Release 12.3.

Workaround; There is no workaround.

- CSCee93804

Symptoms: When you enter the **shutdown** command followed by the **no shutdown** command on the POS interface of an ISE OC-48 line card, a ping or traffic may fail even though the line protocol is up.

Conditions: This symptom is observed on a Cisco 12000 series that is configured for HDLC encapsulation, that does not have keepalives configured, and that has the **pos ais-shut** command enabled. configured.

Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the connected interface at the remote end.

First Alternate Workaround: Disable the **pos ais-shut** command.

Second Alternate Workaround: Configure keepalives.

- CSCee95978

Symptoms: A Cisco router may reload unexpectedly with a Bus error exception.

Conditions: This was observed on a Cisco 7200 series router with an NPE-G1 that was actively passing traffic.

Workaround: There is no workaround.

- CSCef00463

Symptoms: Interoperability problems may occur when you send an L2TPv3 layer 2 specific sublayer AVP by using IETF AVP Type 47.

Conditions: This symptom is observed because Type 47 is assigned by IANA in RFC3308 for the CCDS AVP.

Workaround: There is no workaround.

- CSCef01537

Symptoms: A VIP may reload because of a bus error when a corrupted FIBIDB is used unchecked by the router.

Conditions: This symptom is observed rarely on a Cisco 7500 series when MQC is configured.

Workaround: Disable the MQC configuration.

- CSCef01689

Symptoms: Transient errors may be generated when you boot a 1-port channelized OC-48/STM-16 (DS3/E3, OC-3c/STM-1c, OC-12c/STM-4c) POS/SDH ISE line card. The errors disappear after some time.

Conditions: This symptom is observed on a Cisco 12000 series when you boot the card line card by reloading either the router or the line card itself. The symptom occurs only when the peer router sends RIPv1 packets.

Workaround: There is no workaround.

- CSCef02239

Symptoms: A traceback occurs on a Cisco 10000 series that boots and the verbosity levels that are associated with **debug fdiag** commands may not be set.

Conditions: This symptom is observed only when you boot a Cisco 10000 series from Bootflash or via a netboot.

Workaround: Re-enter the **debug fdiag** commands to set the correct verbosity levels.

- CSCef03176

Symptoms: A ping between two GRE interfaces may not work.

Conditions: This symptom is observed when a GRE tunnel between two routers is up and you ping from the GRE interface of one router to the GRE interface of the other router.

Workaround: There is no workaround.

- CSCef03820

Symptoms: The **set qos group group-id** command does not function on an MPLS-to-IPv6 path.

Conditions: This symptom is observed on a Cisco 12000 series that functions as a 6PE router and that performs hardware forwarding for 6PE traffic.

Workaround: There is no workaround.

- CSCef04163

Symptoms: The subinterface of a link bundle member is not deleted when you reload microcode onto (or perform an OIR of) the line card on which the channel group is configured.

Conditions: This symptom is observed on a Cisco 12000 series when a large number of subinterfaces are configured on a port channel, when you remove a member from the channel group, and when you immediately afterwards reload microcode onto the line card. After the line card has come up, you cannot add members to the channel group until all the subinterfaces of the removed member are deleted. This situation occurs because of a race condition.

Workaround: Wait for a few seconds after you remove a member from the channel group before you reload microcode onto the line card.

- CSCef04202

Symptoms: A QPPB-based service policy that is applied to an ATM interface may stop functioning, and traffic will no longer match the class map.

Conditions: This symptom is observed when you reload a Cisco 10000 series that has QPPB configured on an ATM PVC.

Workaround: There is no workaround.

- CSCef05857

Symptoms: Cache error reporting does not function for SiByte processors, and messages similar to the following misleading error messages are displayed on the console:

```
Invalid CPU type 1 Address: 0x00000000 not in TLB
```

Conditions: This symptom is observed when an L2 cache error occurs on an Sibyte processor such as an NPE-G1.

Workaround: There is no workaround.

- CSCef06050

Symptoms: IPv6 unicast and multicast traffic may not recover on an Engine 4 plus (E4+) 1x10 GE line card after you have performed two software OIRs of the primary CSC.

Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of Cisco IOS Release 12.0S.

Workaround: Reload the E4+ 1x10 GE line card.

- CSCef06121

Symptoms: An Engine 2 3-port Gigabit Ethernet line card may stop transmitting packets.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(24)S6.

Workaround: Enter the **hw-module reload** command to enable the line card to resume transmitting packets.

- CSCef06848

Symptoms: Packets are not load-balanced between interfaces of different POS line cards or POS port adapters.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(25)S or Release 12.0(26)S2 and that has two BGP peers. Four static routes are configured on interfaces of one POS line card or POS port adapter to the loopback IP address of one BGP peer and another four static routes are configured on interfaces of another POS line card or POS port adapter to the loopback IP address of the other BGP peer.

In this configuration, 85 percent of the traffic runs via the output interfaces on one POS line card or POS port adapter. When you enter the **clear adjacency** command, 85 percent of the traffic runs via the output interfaces on the other POS line card or POS port adapter.

Workaround: There is no workaround.

- CSCef08388

Symptoms: After a forced switchover, if you shut down a POS interface and save the configuration, the **shutdown** command does not show for this interface in the output of the **show running-config** command even though the output of the **show ip interface brief** shows that this interface is in the DOWN/DOWN state.

Conditions: The symptom is observed on a Cisco 12410 and Cisco 12416 that run Cisco IOS Release 12.0(25)S4. The symptom does not occur for a Gigabit Ethernet interface.

Workaround: There is no workaround.

- CSCef08774

Symptoms: Certain types of fragmented packets are dropped when the ingress line card is an E6 line card and the egress line card is an E4+ line card. (CSCed22100 addresses this symptom for the E4+ line card.)

Conditions: This symptom is observed on a Cisco 12000 series when there is an Engine 1 GE line card along the path before the traffic enters the E6 line card and when this Engine 1 GE line card does not have any features enabled.

Workaround: Configure a feature such as Sampled NetFlow on the Engine 1 GE line card.

- CSCef09884

Symptoms: The RP that is supposed to become the primary RP may crash when an RP switchover occurs.

Conditions: This symptom is observed on a Cisco 12000 series that runs a Cisco IOS interim release of Release 12.0(26)S3. This caveat is resolved in Release 12.0(26)S3.

Workaround: There is no workaround.

- CSCef10659

Symptoms: The console log of a Cisco 10000 series may contain tracebacks.

Conditions: This symptom is observed when a new configuration is loaded onto the router.

Workaround: There is no workaround. Ignore the tracebacks.

- CSCef11214

Symptoms: An Engine 2 Quad OC-12 POS line card release may fail when it is processing traffic.

Conditions: This symptom is observed on a Cisco 12000 series that runs a Cisco IOS interim release of Release 12.0(26)S3. This caveat is resolved in Release 12.0(26)S3.

Workaround: There is no workaround.

- CSCef11773

Symptoms: A Gigabit Ethernet (GE) subinterface on a 4-port GE line card may use an incorrect destination MAC address, which can be seen in the output of the **show adjacency detail** command.

Conditions: This symptom is observed on a Cisco 12000 series.

Workaround: There is no workaround.

- CSCef12828

Symptoms: When traffic passes through a router, the router blocks traffic for certain prefixes behind a port-channel link. Traffic that originates from the router itself (that is, process-switched traffic) works fine.

Conditions: This symptom is observed on a Cisco 12410 that runs Cisco IOS Release 12.0(27)S1 and that is configured with two PRP-2 processors.

Workaround: There is no workaround.

- CSCef12849

Symptoms: The RP of a Cisco 7500 series that functions as a PE router may crash when you send a ping packet from a CE router that is connected to the PE router to another CE router.

Conditions: This symptom is observed on a Cisco 7500 series that is connected to the CE router via an Ethernet interface.

Workaround: There is no workaround.

- CSCef13024

Symptoms: An Engine 2 line card that is installed in a Cisco 12000 series does not forward packets that are destined for a default route in the hardware. Instead the packets are routed through the line card CPU.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(27)S2.

Workaround: There is no workaround. Traffic goes through the local CPU and so the performance may be affected.

- CSCef14150

Symptoms: The **show policy-map interface** command and its corresponding MIB, CISCO-CBQOS-MIB, report no or fewer Random Drops than what the router actually drops.

Conditions: This symptom is observed only on interfaces that are capable of processing traffic at or faster than 500 Mbps.

Workaround: There is no workaround.

- CSCef15094

Symptoms: When a large policy map is defined, all line cards crash.

Conditions: This symptom is observed on a Cisco 12000 series but may also occur on other platforms.

Workaround: There is no workaround.

- CSCef16326

Symptoms: When you remove a policy map from a subinterface, the subinterface may become stuck, preventing traffic from passing through the subinterface.

Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.0(25)SX7 when a nested policy map is applied to the main or physical interface in addition to the one that is already applied to the subinterface. The symptom could also occur in Release 12.0S.

Workaround: Remove the policy map from the physical interface before you remove the policy map from the subinterface. When the subinterface configuration is updated, re-apply the policy map to the physical interface.

- CSCef20602

Symptoms: A static route to a default route that points at a non-directly connected next hop (a recursive route) may not be properly downloaded to the hardware CEF entry on an Engine 6 line card.

Conditions: This symptom is observed on a Cisco 12000 series.

Workaround: Configure the default route to point to a directly-connected next hop.

- CSCef20651

Symptoms: Pings with the ToS bits set to 00, 10, 1F, 20, 2F, 30, 3F.... E0, EF, F0, or FF function fine but pings with any other ToS bit values fail.

Conditions: This symptom is observed in a configuration in which one CE router connects to a Cisco 10000 series that functions as a PE router and that connects via a Gigabit Ethernet interface to another Cisco 10000 series that also functions as a PE router. This PE router connects, in turn, to another CE router. The pings drop when tag disposition occurs, but not when imposition occurs.

Workaround: There is no workaround.

- CSCef20996

Symptoms: An SNMP query on cbQosREDClassCfg objects may take up a very large part of the CPU utilization of a router. Depending on the overall CPU utilization and query frequency, some side effects such as CPU hogs may occur.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0 S.

Workaround: There is no workaround.

- CSCef21262

Symptoms: An MPLS static label that is configured as an outgoing label is not installed in the MPLS forwarding table.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(29)S when a static label is assigned as an outgoing label for a FEC by entering the **mpls static binding ipv4 prefix mask output nexthop label** command. The statically configured outgoing label is not installed in the MPLS forwarding table.

Note that a static label that is assigned as a local label is properly installed in the MPLS forwarding table.

Workaround: Configure an LDP session to the next hop router over the next hop interface, and configure the next hop router to prevent it from advertising the label for the impacted prefix by entering the **mpls ldp advertise-labels** command.

- CSCef22069

Symptoms: On a Cisco 12000 series that functions as an egress PE router in an MPLS VPN network, after the customer-facing Gigabit Ethernet line card is reloaded, the ingress line card that receives an incoming VPN label with a destination with a glean adjacency (which requires an ARP) without a BGP session may not properly complete the adjacency, causing traffic to be dropped.

Conditions: This symptom is mostly observed with static recursive route configurations. To recover from the symptom, manually ping the interface of the CE router from the adjacent PE router.

Workaround: Configure the static ARP entries for the nexthop router that is configured in the static recursive routes.

- CSCef22498

Symptoms: When MPLS VPN is configured over IP tunnels and IP packets of a certain size (for example, 41 bytes) pass via the tunnel, the following error messages are generated on the customer facing interface (CFI) of a line card:

```
%EE48-3-BM_ERRS: ToFab BM PLIM error 2000 %EE48-3-BM_ERR_DECODE: ToFab PLIM
radar_plim_max_len_err
```

These errors are followed by a reset of the hardware forwarding engine, and the line card stops responding to fabric pings.

Conditions: This symptom is observed on a Cisco 12000 series when MPLS VPN is configured over IP tunnels.

Workaround: There is no workaround.

- CSCef23821

Symptoms: Packet latency in a priority class is high when shaping is enabled in the parent class. For example, when you send 400 kbps of traffic through the priority class, the measured latency is about 80 ms.

Conditions: This symptom is observed when the service policy has a shape average of 768000 on the class default and a child policy with a priority feature.

Workaround: There is no workaround.

- CSCef24642

Symptoms: The PXF engine on a Cisco 10720 may crash, and the following error messages are generated in the logging buffer (the PXF crashinfo files can be found in the flash memory of the router):

```
MSD: %TOASTER-2-FAULT: T0 IHB Exception: watchdog
```

```
MSD: %TOASTER-2-FAULT: T1 IHB Exception: watchdog
```

```
MSD: %TOASTER-2-FAULT: T0 IHB Exception: watchdog
```

```
MSD: %TOASTER-2-FAULT: T1 IHB Exception: watchdog
```

In addition, there are four ways to verify that the symptom is occurring:

- If the **debug main error**, **debug uplink error**, and **debug access error** commands are enabled on the router, the following error messages are also generated in logging buffer:

```
MSD: %Camr_SRP_OC48-3-INTERR: SRP uplink internal error SRP_TX_VA_SC_GIANT_PKT (code 4)
```

```
MSD: %Camr_SRP_OC48-3-INTERR: SRP uplink internal error SRP_TX_VA_SC_FIFO_GIANT_PKT (code 100)
```

```
MSD: %Camr_VA-3-STATUS1: Van Allen Data integrity error VA_SC_IPM_RD_ACC_TIMER_EXP (code 1)
```

```
MSD: %Camr_VA-3-STATUS1: Van Allen Data integrity error VA_RP_IPM_RD_ACC_TIMER_EXP (code 4)
```

```
MSD: %Camr_VA-3-SISTATUS: Van Allen SRIC Data integrity error VA_SI_FL_CTRL_DRV (code 80)
```

```
MSD: %Camr_VA-3-SOSTATUS: Van Allen SROC Data integrity error VA_SO_PKT_LEN_ERR (code 1)
```

```
MSD: %Camr_VA-3-STATISTICS: VA statistics register: 0x0098 reports VA_SO_PKT_LEN_ERR_COUNT = 3
```

- In the output of the **show interface srp 1/1** command, the received error counters such as “framer runs” and “input errors” have a large value.
- In the output of the **show hard pxf cpu statistics interface srp 1/1 detail** command, the “destination unreachable” counter increases.
- In the output of the **show hard pxf cpu statistics interface srp 1/1 detail** command, the “zero encap length” counter increases.

Conditions: This symptom is observed when all of the following conditions are present:

- A packet enters with or without an MPLS label.
- The router tries to send an ICMP packet to the source in any of the following situations:
 - * The packet is denied by an output security ACL.
 - * There is no route in the router to forward the packet.

- * The time to live (TTL) of the packet expires.
- * The packet is an ICMP echo request packet, and the router tries to send an ICMP echo reply packet to the source.
- On the interface on which the packet enters, the **ip unreachable** command is enabled by default.

Workaround: Enter the **no ip unreachable** command on all interfaces of the router, which works in the following two cases:

- The packet is denied by an output security ACL.
- There is no route in the router to forward the packet.

For other cases, there is no workaround.

- CSCef24843

Symptoms: A Cisco 12000 series may crash and hang.

Conditions: This symptom is observed on a Cisco 12000 series that runs a bootloader image of a Cisco IOS interim release for Release 12.0(30)S and that is configured with a PRP-1. However, this caveat is resolved in Release 12.0(30)S.

Workaround: There is no workaround.

- CSCef25866

Symptoms: Connectivity for destinations that are reachable via an MPLS TE tunnel may fail when the tunnel is fast-rerouted. The loss of connectivity may result in loss of TCP sessions (BGP, LDP, etc.) for those destinations.

When the problem happens, the output of the **show ip cef network** command shows “invalid cached adjacency” for the tunnel but does not show “fast tag rewrite.”

Conditions: This symptom is observed when all of the following conditions are present:

- The adjacency of the primary tunnel becomes incomplete when FRR is active, as can be observed in the output of the **show adjacency type number** command. Whether or not the adjacency becomes incomplete is media-dependent. For example, with PPP the adjacency becomes incomplete but not with HDLC.
- The primary tunnel is the only path to reach the prefix in question.
- The **ip cef accounting non-recursive** command is not enabled.
- A routing change occurs for the prefix after the FRR switchover. (This is topology dependent)

Workaround:

- Use HDLC encapsulation instead of PPP. This will prevent the adjacency from becoming incomplete.
- Use forwarding adjacencies. This will prevent the routing change.

Further Problem Description: The symptom affects traffic that originates on the tunnel headend. Transit traffic going through the tunnel is not affected. The symptom does not occur if there are multiple paths to the destination (one of which is the tunnel).

- CSCef25872

Symptoms: An OC192E/POS-IR-SC line card in a Cisco 12000 series may crash with the following messages:

```
%GRP-4-RSTSLOT: Resetting the card in the slot: 4,Event: linecard error report
%MDX-1-DAEMSGSNDFAILED: FAILED to send IPC message of TYPE MDX_DAE_PULL_REQ to
slot 4 on the DAE,
      FAIL REASON = retry queue flush
```

%LCINFO-3-CRASH: Line card in slot 4 crashed

Conditions: The symptom is seen when the ciscoOpticalMonitoringMIB is polled on a router running Cisco IOS Release 12.0(27)S1. The card that crashes does not have to be the card that is being polled. For example, an OC192E/POS-VSR in slot 0 may be polled with 1.3.6.1.4.1.9.10.83.1.1.1.1.8.2 and the OC192E/POS-IR-SC in slot 4 may crash.

Workaround: Stop the crashes by configuring an SNMP view that prevents the ciscoOpticalMonitoringMIB from being polled.

- CSCef25953

Symptoms: DSCP-based DWRED statistics are not updated in output of the **show policy-map interface** command; random drop and tail drop statistics are always shown as zero.

Conditions: This symptom is observed on a Cisco 7500 that is configured with an RSP4. However, this caveat may be platform-independent.

Workaround: There is no workaround.

- CSCef26053

Symptoms: Load-balancing does not work over a BGP multipath. Some of the traffic may be forwarded correctly while other traffic may be forwarded unlabeled into the MPLS core.

Conditions: This symptom is observed on a Cisco router that functions as a PE router when the following conditions are present:

- The affected route is in a VRF.
- One of the paths is learned from a CE router via an eBGP multihop session.
- The eBGP multihop peer (that is, the CE router) is reachable through the MPLS core and the BGP session does not involve a label exchange.

Workaround: Avoid a multihop eBGP session in which the CE router is reachable through the MPLS core. For example, instead of a configuration in which the CE router connects to the PE router across the MPLS core, configure the CE peer to connect to a local PE router that redistributes the routes it has learned from the CE peer to other PE routers. (The local PE router may need to be configured for eiBGP multipath.)

- CSCef26077

Symptoms: Unconfiguring link bundling on a GE interface causes a bus error on the RP.

Conditions: This symptom is observed on a Cisco 12000 series that runs a Cisco IOS interim release of Release 12.0(30)S. However, this caveat is resolved in Release 12.0(30)S.

Workaround: There is no workaround.

- CSCef26186

Symptoms: After a router reloads, Engine 0 POS and Engine 4+ POS line cards may reset because of an “%MDS-2-LC_FAILED_IPC_ACK” error.

Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of an interim release for Cisco IOS Release 12.0(30)S and that has multicast enabled in global configuration mode. Note, however, that this caveat is resolved in Release 12.0(30)S.

Workaround: There is no workaround.

- CSCef26370

Symptoms: When you copy a Cisco IOS image or any other file to a PC flash card via TFTP, a very high rate of out-of-sequence packets occurs, which can be seen in the “!0!00!0!00!0!0...” output of the **copy tftp slot-number** command.

The image or file is copied over successfully to the PC flash card, but it takes about three times longer than usual.

Conditions: This symptom is observed on a Cisco platform that has a processor that runs at a low speed.

Workaround: If the file is small, it may be copied to bootflash. There is no other workaround.

- CSCef27191

Symptoms: It is not possible to change the duplex configuration to full duplex on a Fast Ethernet (FE) interface of a Cisco 7200 series. When you enter the **full-duplex** interface configuration command, the command is ignored. The parser accepts the command, but it is not shown in the output of the **show running-config** command and the output of the **show interface** command shows the FE interface as half-duplex.

Conditions: This symptom is observed when the FE interface belongs to a PA-2FEISL-FX or PA-2FEISL-TX port adapter and when the Cisco 7200 series runs Cisco IOS Release 12.0(28)S or a later release.

Workaround: There is no workaround.

- CSCef27197

Symptoms: OAM emulation does not function on an interworking connection.

Conditions: This symptom is observed when OAM emulation is enabled on an AAL5 connection between a CE router and a PE router when this AAL5 connection is configured for interworking. The PE router receives the OAM cells but drops them, and the ATM PVC on the CE router is down.

Workaround: There is no workaround.

- CSCef27580

Symptoms: Policy-based routing (PBR) loadsharing does not occur.

Conditions: This symptom is observed on a Cisco 12000 series when PBR loadsharing is enabled via the **set next-hop recursive** command and when routes to the destination are available via multiple interfaces. When you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface that connects to the next-hop (or when the interface goes down and comes back up), traffic does not resume on this interface.

Workaround: Enter the **static arp** command on the interface that connects to the next-hop.

- CSCef27796

Symptoms: A router may crash when you create an ATM subinterface.

Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS interim release for Release 12.0(30)S when you quickly create an ATM subinterface and enter the **mpls ip** command on the interface. Note that this caveat is resolved in Release 12.0(30)S.

Workaround: There is no workaround.

- CSCef28765

Symptoms: An error message similar to the following one (in which the tunnel interface is a Generic Routing Encapsulation [GRE] tunnel) and a traceback may be generated:

```
%IPFAST-2-PAKSTICK: Corrupted pak header for Tunnel18, flags 0x20
```

In addition, connectivity problems may occur.

Conditions: These symptoms are observed on a router that runs Multiprotocol Label Switching (MPLS) over a GRE tunnel and that advertises an explicit null label.

Workaround: Do not use an explicit null label. Rather, use the default implicit null label.

- CSCef28848

Symptoms: The following error message is generated repetitively for an ATM OC-12 line card:

```
%FIA-3-REQUESTERR: Request error was detected. Type = 1
```

The output of the **show controller fia** command shows that the “Empty dst request” field continues to increment for the line card, and the line card is unable to pass multicast traffic.

Conditions: This symptom is observed on a Cisco 12000 series when multicast packets do not have their Cisco cell fields properly set.

Workaround: There is no workaround.

- CSCef29467

Symptoms: When you enter commands in various configuration modes such as address-family, PVC, service-policy, and so on, an invalid input error message may be returned even though the command was accepted and entered into the running configuration. The following is an example:

```
Router(config-router-af)#redistribute connected
address-family ipv4 vrf atmTrk
^
```

Invalid input detected at “^” marker.

Conditions: This symptom is observed on a Cisco 12410 that is configured with two Performance Route Processors (PRP-1) that function in Route Processor Redundancy (RPR) mode and that runs one of the following images:

- The c12kprp-p-mz image of Cisco IOS Release 12.0(24)S3.
- The c12kprp-p-mz image of Cisco IOS Release 12.0(23)S4.
- The c12kprp-k3p-mz image of Cisco IOS Release 12.0(27)S2

This list is not all-inclusive: the symptom may also occur in Release 12.0(20)S, Release 12.0(20)ST, and later releases.

The symptom occurs when the **do** command is interleaved between configuration commands.

Workaround: Verify that the configuration command is properly accepted by entering the **show running-config** command.

- CSCef30166

Symptoms: A Cisco router does not bring down a FR PVC when the interface on the ATM side is shut down.

Conditions: This symptom is observed on a Cisco router that runs an interim release for Cisco IOS Release 12.0(30)S only when OAM is configured on the ATM side.

Workaround: There is no workaround.

- CSCef30180

Symptoms: A cell-packing configuration may not be added to a PVC.

Conditions: This symptom is observed when cell packing is configured on an ATM interface.

Workaround: There is no workaround.

- CSCef31649

Symptoms: A VRF interface receives auto-RP discovery packets only once via the core link. After that, no more RP discovery packets are received. After three minutes, the RP mapping table ages out, preventing multicast traffic from being passed.

Conditions: This symptom is observed on a Cisco 12000 series that has hardware-enabled multicast configured on a VRF interface.

Workaround: Disable hardware multicast on the VRF interface.

- CSCef31934

Symptoms: In a scaled configuration with hundreds of eBGP peers with very low BGP timers, issuing **clear ip bgp *** may increase HW forwarding memory utilization.

Conditions: This problem is seen with 500 eBGP sessions with BGP keepalive timer of 3 seconds and hold timer of 9 seconds. The router has 200K MPLS VPN routes. This problem is not seen if the BGP timers are set to the default value.

Workaround: There is no workaround.

- CSCef33670

Symptoms: An Engine 4 egress line card that switches traffic may reset when the ingress line card is shut down.

Conditions: This symptom is observed on a Cisco 12000 series when the ingress line card is an Engine 3 POS line card and when IP-to-tag traffic is switched.

Workaround: There is no workaround.

- CSCef37127

Symptoms: When you connect a Cisco 10000 series 4-port channelized STM-1/OC-3 line card to another device, DS3 port 2 and 3 report that the AIS is stuck in the down/down state. When you connect a loopback fiber to the 4-port channelized STM-1/OC-3 line card, DS3 port 2 and 3 come back up.

Conditions: This symptom is observed when the 4-port channelized STM-1/OC-3 line card is configured for SONET-to-DS3 mapping and when you connect the line card to another device (that is not another 4-port channelized STM-1/OC-3 line card).

Workaround: Because the 4-port channelized STM-1/OC-3 line card transmits a multiframe alignment in the H4 overhead byte, configure the other device to generate an H4 multiframe alignment.

Further Problem Description: The 4-port channelized STM-1/OC-3 line card detects a loss of multiframe alarm and generates an AIS downstream towards the DS3 framers. Multiframe alignment is not present for DS3-based mappings into SONET. This situation causes the DS3 ports to go down when they receive the inappropriate alarm.

- CSCef37716

Symptoms: An LSP ping may not interoperate with third-party vendor equipment. The following commands may either timeout or receive an error return code from third-party vendor equipment:

- **ping mpls ipv4** *ip-address address-mask*
- **trace mpls ipv4** *ip-address address-mask*
- **ping mpls pseudowire** *peer-id vc-id*

Conditions: This symptom occurs because of recent changes to the ietf-mpls-lsp-ping-06.txt draft, preventing Cisco's implementations of LSP pings from interoperating with third-party vendor equipment.

The recent draft changes include the following:

- “Implicit padding” of the Target FEC TLV subtype lengths is required when pinging an LDP IPV4 FEC.
- The FEC definition that is used in the **ping mpls pseudowire** command now requires Target FEC TLV subtype 10 instead of 9.

Workaround: There is no workaround.

- CSCef39284

Symptoms: A router may crash when you enter the **crypto key generate dss** *key-name* command.

Conditions: This symptom is observed on a Cisco 12012 that is configured for SSH but may occur on any Cisco platform that is configured for SSH.

Workaround: There is no workaround.

- CSCef39381

Symptoms: When 1000 input ACLs are configured on an Engine 3 line card and when traffic is denied by the input ACL, the following error message and traceback are displayed continuously on the console:

```
%GRP-4-NO_INTF: CSAR: No interface available Slot 4 Chan 19
-Traceback= 1ADD94 44A2E4 44A988 44BD94 44C3D0 4451D8 27CCB0
```

This symptom occurs whether the router is configured with a GRP, a PRP-1, or a PRP-2. When the router is configured with a PRP-1 or PRP-2, the output of the **show controllers psar | incl idb** shows the following:

```
No IDB drops - 3423 IDB queue tail drops - 0 CORE2-R2#
```

However, the output of the **show idb** command shows that there are 32 IDBs.

When the router is configured with a GRP, the output of the **show controllers csar** does not show anything unusual.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(27)S1 or Release 12.0(27)S2a only when an input ACL is applied, when traffic is denied by the input ACL, and when the **ip unreachable** command is enabled on the interface of the Engine 3 line card.

Workaround: Enter the **no ip unreachable** command on the interface of the Engine 3 line card.

- CSCef40001

Symptoms: When the **police cir percent** command is configured as a service-policy input on an MFR or MLP bundle CFI, the maximum bandwidth that is allocated by the service policy is a T1 link bandwidth.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(28)S or an interim release for Release 12.0(30)S when a police-policy input is applied on the bundle CFI over a 1-port OC-12 channelized ISE line card. Note, however, that this caveat is resolved in Release 12.0(30)S.

Workaround: There is no workaround.

- CSCef40187

Symptoms: An SRP interface is stuck and there is no response at all. In the output of the **show srp topology** command, the last topology packet that is received takes more than five seconds to arrive. In addition, the “zero encap length” counter in the output of the **show hardware pxf cpu stat interface srp 1/1 detail** command increases.

Conditions: This symptom is observed on a Cisco 10720 when the value of the overall packet size divided by 32 is 1 or 2.

Workaround: There is no workaround.

- CSCef41460

Symptoms: A generic routing encapsulation (GRE) tunnel may not work on a provider edge (PE) router if VPN is configured.

Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of Cisco IOS Release 12.0(25)S or a later release.

Workaround: There is no workaround.

- CSCef42433

Symptoms: When port 0 of an ESR-4ATMOC3 line card has some PVCs configured and you perform an OIR of this line card, all the PVCs under port 1, port 2, and port 3 enter the inactive state.

Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.0(27)S or 12.0(28)S.

Workaround: There is no workaround.

- CSCef42706

Symptoms: CPUHOG conditions, BGP sessions flaps, and APS channels flaps are observed on a router.

Conditions: These symptoms are observed when SNMP is polled on a Cisco 12000 series that has about 500 interfaces and subinterfaces and more than 900 attached service policies. The router may produce CPUHOG log messages when the CISCO-CLASS-BASED-QOS-MIB stats are polled.

Workaround: There is no workaround.

- CSCef42815

Symptoms: A flap of the BGP session between a primary provider edge (PE) router and a customer edge (CE) router that provides the default route may cause a remote CE router to lose Internet connectivity when the BGP session is restored.

Conditions: This symptom is observed in a topology with CE routers that are dual-homed and connected to two Cisco 12000 series routers that function as PE routers and that run Cisco IOS Release 12.0(26)S2 when the default route is generated by a CE router in a different VPN routing/forwarding (VRF).

Workaround: There are two steps to the workaround:

1. Add a default VRF static route to cover the BGP-derived default route.
2. Clear the default route entry in the routing table.

- CSCef42849

Symptoms: In a PRE-1 and PRE-2, a timing violation occurs in the third-party vendor temperature sensor, causing the temperature reading to fail.

Conditions: This symptom is observed in a Cisco 10000 series PRE-1 and PRE-2. Old-type temperature sensors are not effected.

Workaround: There is no workaround.

- CSCef43691

A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP "hard" error messages.

2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks.
3. Attacks that use ICMP “source quench” messages.

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml>.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected.

- CSCef44154

Symptoms: When an MPLS packet that enters through an SRP or Ethernet interface contains an L2TP or UTI packet and this MPLS packet is processed by the RP instead of the PXF engine (for example, when the IP header in the MPLS packet contain options and the MPLS TTL equals 0 or 1), the SRP or Ethernet interface stops receiving packets.

Conditions: This symptom is observed on a Cisco 10720 that runs Cisco IOS Release 12.0S.

Workaround: There is no workaround.

- CSCef44274

Symptoms: The per-WRED-class drop counters do not increment in the output of the **show queueing** command even though there are aggregate WRED drops.

Conditions: This symptom is observed when the **random-detect** legacy command is enabled on the main interface.

Workaround: Attach a policy map that has the **random-detect** legacy command enabled to the interface.

- CSCef45609

Symptoms: An Engine 3 Quad OC-12 line card that is configured with multicast VPNs may punt traffic to the RP when multicast is disabled by entering the **no ip multicast-routing distributed** command and then re-enabled by entering the **ip multicast-routing distributed** command.

Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of Cisco IOS Release 12.0(26)S4 or a later release but may also occur in other releases.

Workaround: There is no workaround.

- CSCef48325

Symptoms: WRED counters do not function on distributed platforms such as a Cisco 7500 series and a Cisco 7600 series.

Conditions: This symptom is observed on a distributed Cisco platform that runs Cisco IOS Release 12.0(26)S3, 12.0(29)S, 12.2(25)S, 12.3(10), or 12.3(11)T and that has dWRED configured.

Workaround: There is no workaround.

- CSCef48573

Symptoms: An Engine 3 Quad OC-12 line card that is configured with multicast VPNs may punt traffic to the Route Processor (RP).

Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of a Cisco IOS interim release for Release 12.0(30)S. Note, however, that this caveat is resolved in Release 12.0(30)S.

Workaround: There is no workaround.

- CSCef49110

Symptoms: When you enter the **dir** command on a disk, the command fails with a “read_file/dir failed” error message.

Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.2S.

Workaround: Format the disk. Note that the fix for this caveat involves a design change and is therefore integrated in various releases.

- CSCef49387

Symptoms: When you first enter the **aps working** command and then enter the **aps group group-number** command, the *group-number* argument is automatically set to zero. Even when you enter the **no aps group group-number** command, you still can not set the *group-number* argument to a value other than zero.

Conditions: This symptom observed on a Cisco 12000 series that runs an interim release for Cisco IOS 12.0(30)S. Note, however, that this caveat is resolved in Release 12.0(30)S.

Workaround: Enter the **no aps working** command. Then, enter the **aps group group-number** command followed by the **aps working 1** command.

- CSCef52144

Symptoms: An active RP crashes after you remove an event manager applet.

Conditions: This symptom is observed on a Cisco 12000 series that runs an interim release for Cisco IOS Release 12.0(30)S. However, this symptom is resolved in Release 12.0(30)S. The symptom may also occur in other releases.

Workaround: There is no workaround.

- CSCef52419

Symptoms: In Cisco IOS software releases earlier than Cisco IOS Release 12.0(27)S3, Release 12.0(28)S1, and Release 12.0(30)S, the CPU utilization of a Cisco 10720 is high (x%/y%, where y is greater than 60 percent), and continuous BGP and LDP flapping is reported. The counters in the output of the **show interface** command show a large number of drops and the output of the **show buffers** command shows a large number of cache misses for the private IBC buffer pools.

Conditions: This symptom is observed when the Cisco 10720 functions in a broadcast ARP storm environment and when the *length* argument of the **hold queue length in** interface configuration command is not the default of 75 packets for any interface of the router (for example, the *length* argument is 2048).

Workaround: Revert the **hold queue length in** interface configuration command and the **hold queue length out** interface configuration command to the default setting on all interfaces with non-default hold queues.

- CSCef52712

Symptoms: The CPU utilization of a Cisco 12000 series may approach 100 percent when a 10,000-line IPv6 ACL is added and removed, and the router may crash.

Conditions: This symptom is observed on a Cisco 12000 series that runs an interim release for Cisco IOS Release 12.0(30)S. Note, however, that this caveat is resolved in Release 12.0(30)S.

Workaround: There is no workaround.

- CSCef52974

Symptoms: An Engine 3 ingress line card crashes continuously with alpha errors and IPC errors when it processes ingress multicast traffic.

Conditions: This symptom is observed on a Cisco 12000 series when you reload an Engine 3 ingress line card that has 5000 (S,G) entries.

Workaround: There is no workaround.

- CSCef53085

Symptoms: The rates that are specified in MQC wrongly include the L1 overhead. For example, if you configure the **bandwidth 100** command, 100 Kbps of L3 + L1 is guaranteed, excluding the L2 overhead. The throughput of L3 is therefore less than 100 kbps. (Note that the L2 overhead is not supposed to be included.)

Conditions: The symptom is observed in Cisco IOS Release 12.0(28)S and earlier releases.

Workaround: There is no workaround.

- CSCef53109

Symptoms: When you enter the **do** command with arguments on an interface member of a port-channel or pos-channel group, a message similar to the following one is displayed:

```
Command "do <arguments>" not allowed on link-bundle member interface
<interface-number>
```

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S when the command is entered on an interface member of a port-channel or pos-channel group.

Workaround: Enter the command directly on the interface that you are querying.

- CSCef53169

Symptoms: An outbound ACL with a log/log-input keyword changes the IP destination address in the packets. As the result, packets that should be permitted are incorrectly denied.

Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.0(29)S when the incoming interface for the packets is a tag-switching interface. The symptom is observed irrespective of whether the interface with this outbound ACL is a tag-switching interface or not.

Workaround: Do not use the log/log-input keyword in the ACL.

- CSCef53475

Symptoms: Packet drops occur when traffic is sent below the shape rate that is defined in a service policy.

Conditions: This symptom is observed on a Frame Relay interface when there are multiple DLCIs that have service policies enabled. Each DLCI has a hierarchical policy with a shape rate in the class default at the parent level and a child policy with LLQ and CBWFQ classes. When traffic to each DLCI is just below the shape rate and the combined traffic through the interface is close to line rate, packet drops occur on some DLCIs. The symptom does not occur when traffic is sent to one DLCI at the time.

Workaround: Increase the shape rate to compensate for the scheduling inaccuracy.

- CSCef53570

Symptoms: When IPv4 multicast is configured on an interface and when hardware forwarding is enabled, the interface stops forwarding all unicast and multicast traffic.

Conditions: This symptom is observed only on Cisco 12000 series Engine 2 line cards.

Workaround: Disable hardware forwarding.

- CSCef54021

Symptoms: After an SSO switchover has occurred, traffic stops on interfaces that have both an input and an output policy attached.

Conditions: This symptom is observed on a Cisco 12000 series.

Workaround: Remove and re-attach the policies to the interfaces.

- CSCef54308

Symptoms: An Engine 4 plus (E4+) interface polices traffic although no policing is configured.

Conditions: This symptom is observed on a Cisco 12000 series when MQC is configured with policing on an E4+ interface and then MQC is removed from the interface.

Workaround: Reload the E4+ line card.

- CSCef54624

Symptoms: The secondary RP of a Cisco 12816 cannot be booted and is stuck in the “RDY RP” state.

Conditions: This symptom is observed on a Cisco 12816 that runs an interim release for Cisco IOS Release 12.0(30)S and is independent of the redundancy modes that is configured (RPP, RPR+, or SSO). The Cisco 12816 is configured with a PRP-1 in slot 0 and a PRP-2 in slot 2. Note that this caveat is resolved in Release 12.0(30)S.

Workaround: There is no workaround.

- CSCef54679

Symptoms: Time-based policing and shaping do not function on a 4-port OC-3 ATM ISE line card.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(28)S when an input service policy is attached to a VC.

Workaround: There is no workaround.

- CSCef54779

Symptoms: Under a rare condition, when a main interface switches over to a backup interface on 4-port GE line card, a ping to another neighboring interface that is not at all related to the backup interface fails. A sniffer trace shows that the Src/Dst MAC address in the ICMP reply is that of the backup interface.

Conditions: This symptom is observed on a Cisco 12000 series when you repeatedly disable the main interface that is associated with a backup interface.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface.

- CSCef54855

Symptoms: A 6-port channelized T3 interface may not come up after booting, and a traceback may be generated.

Conditions: This symptom is observed on a Cisco 10000 series that runs a Cisco IOS interim release for Release 12.0(30)S. However, this caveat is resolved in Release 12.0(30)S.

Workaround: There is no workaround.

- CSCef55373

Symptoms: The BGP process can take up 100 percent of the CPU for an extended period of time when 6PE is configured.

Conditions: This symptom is observed on a Cisco 12000 series when a large number of IPv6 routes and 6PE labels are allocated.

Workaround: There is no workaround.

- CSCef55463

Symptoms: When you configure vbr-nrt shaping on two or more PVCs that are defined under the same physical ATM interface, one of the PVCs is subsequently unable to achieve the configured vbr-nrt rate.

Conditions: This symptom is observed when a PA-A3-8E1IMA or PA-A3-8T1IMA port adapter is installed in a Cisco 7xxx series and when the load is equal to or greater than the maximum configured vbr-nrt rate on at least two PVCs.

Workaround: Configure vbr-nrt rates proportionally higher on each PVC. Enter the **transmit-priority 1** command on the PVC that must reach the guaranteed vbr-nrt. Doing so causes the other PVC or PVCs to reach approximately 90 to 95 percent of the configured vbr-nrt rate.

- CSCef56116

Symptoms: If the VLAN IDs on either side of an AToM cloud are different, the imposition side is supposed to rewrite the VLAN ID with the remote value; this functionality does not work.

Conditions: This symptom is observed on a Cisco 12000 series that functions in an AToM VLAN-to-VLAN environment.

Workaround: There is no workaround.

- CSCef56327

Symptoms: You may not be able to configure the **clock source line** command during the configuration of the SONET controller on a Cisco 7200 series in which a PA-MC-STM1 port adapter is installed.

When you enter the **clock source line** command during the configuration of the SONET controller, the output of the **show running-config** command indicates that the clock source is set to line. However, the output of the **show controllers sonet** command indicates that the clock is set to internal, and when you enter the **show running-config** command again, the output indicates this time that the clock source is set to internal.

Conditions: This symptom is observed when the PA-MC-STM1 port adapter is connected back-to-back via dark fiber to another PA-MC-STM1 port adapter.

Workaround: Enter the **overhead s1byte ignore** command on the SONET controller before you configure the clock source.

- CSCef56758

Symptoms: The **cell packing** command can not be configured under a vc-class template.

Conditions: This symptom is observed on a Cisco platform that runs a Cisco IOS release that is listed in the “First Fixed-in Version” field at <http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCdv49909>. Releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

Workaround: There is no workaround.

- CSCef57272

Symptoms: Even though the **hw-module slot-number tcam compile no-merge** command is enabled, per-ACE counters in the output of the **show access-lists** command do not increment when the same ACL is applied to more than one port.

Conditions: This symptom is observed on a Cisco 12000 series when the same ACL is applied to more than one port. Note that aggregate counters work fine. The symptom does not occur when the ACL is applied to a single port.

Workaround: There is no workaround.

- CSCef59140

Symptoms: The protocol may go down on random link bundles that are part of the multilink Frame Relay (MFR) protocol on a Cisco 12000 series that is configured with a channelized OC-12 DS1 line card.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S after you have reloaded the router.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected link bundles.

- CSCef59275

Symptoms: Prefixes are rewritten over a FRR backup tunnel, causing traffic to drop from the tunnel.

Conditions: This symptom is observed when a point of local repair (PLR) runs Cisco IOS Release 12.0(29)S and the merge point (MP) runs a release earlier than Release 12.0(29)S or Release 12.2S.

Workaround: Run Release 12.0(29)S or a later release on the MP.

- CSCef59972

Symptoms: An RP crashes when you remove class maps from a policy map.

Conditions: This symptom is observed on a Cisco 12000 series that runs a Cisco IOS interim release for Release 12.0(30)S.

Workaround: There is no workaround.

- CSCef61054

Symptoms: When you configure an inter-area LSP, metrics, attributes, or both are not signaled, causing the LSP to follow an unexpected and possibly undesired path.

Conditions: This symptom is observed on a Cisco router that is configured for MPLS TE.

Workaround: There is no workaround.

- CSCef61641

Symptoms: A change in the controller state does not affect the subrate interface state.

Conditions: This symptom is observed on a Cisco 7500 series that is configured with an PA-MC-2T3+ port adapter.

Workaround: There is no workaround. However, you can synchronize the interface with the controller by entering the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface.

- CSCef62246

Symptoms: An Auto-RP mapping entry may expire when hardware acceleration is enabled on the VRF interfaces or when a static VRF RP statement is configured on the PE router.

Conditions: This symptom is observed on a Cisco 12000 series that functions as a PE router.

Workaround: Disable hardware acceleration or define a static VRF RP statement with an ACL.

- CSCef64254

Symptoms: When there is a large MQC configuration, a Route Processor (RP) may crash because of lack of memory.

Conditions: This symptom is observed on a Cisco 12000 series that is configured with ISE line cards when you add a large number of classes to a policy map that is attached to a large number of subinterfaces.

Workaround: There is no workaround.

- CSCef64744

Symptoms: On a 6-port channelized T3 line card that is enabled for QoS, a low latency queue (LLQ) may not receive traffic that is mapped to the LLQ.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S1.

Workaround: Reload the line card. If this is not an option, there is no workaround.

- CSCef66449

Symptoms: A PE router that functions in an EoMPLS environment may crash.

Conditions: This symptom is observed on a Cisco 10720 when 1200 circuits are configured in port transparency mode.

Workaround: There is no workaround.

- CSCef66517

Symptoms: When you send larger than fragment-sized packets from an interface that has a traffic shaping class configured, the packets get stuck when the queue size increases to the queue limit, and subsequent traffic is tail-dropped.

Conditions: This symptom is observed when a policy is attached to a multilink interface that has a traffic shaping class configured and when the interface is configured for fragmentation.

Workaround: There is no workaround.

- CSCef66562

Symptoms: The cbQosPolicyMapName object may stop functioning.

Conditions: This symptom is observed when an active view includes the ciscoPingMib.

Workaround: Either remove the ciscoPingMib or include the **system** keyword in the same view by entering the **snmp-server view PingMIB system included** command.

- CSCef67078

Symptoms: A PXF buffer leak occurs on an L2TPv3 decapsulation router, which can be observed in the output of the **show hardware pxf cpu buffer** command:

```
router#show hardware pxf cpu buffer
FP buffers
pool    size    # buffer    available    allocate failures    low buffer drops
-----
0       9344    1293        1293         0                    0
1       1664    12930       12930        0                    0
2        640    26746       127          0                    77165
3        256    34072       34072        0                    0
4        128    59934       59934        0                    0
```

Depending on the packet size, the buffer leak can occur in different pools.

Conditions: The symptom is observed on a Cisco 10720 in the following two scenarios:

- An MPLS-enabled interface is the network backbone for L2TPv3 tunnels.
- An 802.1q interface is the network backbone for L2TPv3 tunnels and an input security ACL with more than 400 lines is configured on the 802.1q backbone interface.

Workaround: There is no workaround.

- CSCef67267

Symptoms: The Fast ReRoute database shows all prefixes in the active state.

Conditions: This symptom is observed on a Cisco router after a connected point of local repair (PLR) has rebooted.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface on which the primary tunnel is configured. Doing so restores the prefixes to the ready state.

- CSCef67911

Symptoms: Multicast traffic stops on a PE router that is configured for mVPN.

Conditions: This symptom is observed on a Cisco 12000 series that functions as a PE router when a default MDT switchover to the data MDT occurs.

Workaround: Clear the VRF mroutes on the affected line card by entering the **clear ip mds vrf vrf-name forwarding** command.

- CSCef68324

Cisco Internetwork Operating System (IOS) software is vulnerable to a Denial of Service (DoS) and potentially an arbitrary code execution attack from a specifically crafted IPv6 packet. The packet must be sent from a local network segment. Only devices that have been explicitly configured to process IPv6 traffic are affected. Upon successful exploitation, the device may reload or be open to further exploitation.

Cisco has made free software available to address this vulnerability for all affected customers.

More details can be found in the security advisory that is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050729-ipv6.shtml>.

- CSCef69146

Symptoms: A Cisco 12000 series crashes when the encapsulation of T1 channels is changed to MFR during a cut-and-paste operation of the configuration or when you copy from a file to the running configuration.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S1 and that is configured with a 1-port channelized OC-12/STM-4 (DS1/E1) ISE line card when the configuration is changed at a fast pace. When the configuration lines are entered at a slower pace, the symptom does not occur.

Workaround: Avoid pasting configuration files to the 1-port channelized OC-12/STM-4 (DS1/E1) ISE line card. If this is not an option, there is no workaround.

- CSCef69631

Symptoms: All line cards may reset and may not enter the “RUN” state after a software OIR or the primary CSC occurs on a Cisco 12000 series that has 40 GB of fabric.

Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of an interim release for Cisco IOS Release 12.0(30)S. However, this caveat is resolved in Release 12.0(30)S.

Workaround: Power cycle the router.

- CSCef70953

Symptoms: An Engine 4+ line card resets when you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on an interface of an Engine 3 Gigabit Ethernet (GE) line card in the same router.

Conditions: This symptom is observed on a Cisco 12000 series that functions in an EoMPLS configuration, that has an Engine 3 Gigabit Ethernet egress line card and an Engine 4+ core-facing line card, and that has CDP is enabled.

Workaround: Disable CDP.

- CSCef72272

Symptoms: A basic VRF ping may not go through.

Conditions: This symptom is observed on a Cisco 12000 series that is configured for MPLS VPN and that has an Engine Gigabit Ethernet line card that is connected to an Engine 4+ line card.

Workaround: There is no workaround.

- CSCef72305

Symptoms: A standby PRE crashes on bootup.

Conditions: This symptom is observed on a Cisco 10000 series that is configured with 1000 ATM VCs when a forced SSO switchover occurs.

Workaround: There is no workaround.

- CSCef72411

Symptoms: Line cards and the standby RP on a Cisco 12000 series may fail when an RP switchover occurs.

Conditions: This symptom is observed on a Cisco 12000 series that runs a Cisco IOS interim release for Release 12.0(30)S and that has two PRPs when you enter the **redundancy force-switchover** command. Note that this caveat is resolved in Release 12.0(30)S.

Workaround: There is no workaround.

Further Problem Description: The fix for this caveat enables the RP to recover from a Fabric Interface ASIC (FIA) halt condition if this condition occurs following an RP switchover. In a Cisco IOS software release that does not integrate the fix for this caveat, the RP does not attempt to recover from a FIA halt condition after an RP switchover has occurred (but it does attempt to recover from such a conditions in other situations).

- CSCef72555

Symptoms: When you change the Cisco IOS software image on a Cisco 10000 series, HA may function differently, causing strange behavior, a standby crash, or both.

Conditions: This symptom is observed when you change the Cisco IOS software image on a Cisco 10000 series from one release train to another release train. This symptom affects Release 12.0S, Release 12.2S, releases that have been derived from Release 12.2 releases, and releases that have been derived from Release 12.3.

Workaround: There is no workaround.

- CSCef77359

Symptoms: If VLAN IDs on either side of an AToM cloud are different, the imposition side is supposed to overwrite its VLAN ID with the remote VLAN ID, but this does not occur.

Conditions: This symptom is observed on a Cisco 12000 series that functions in an AToM VLAN-to-VLAN environment.

Workaround: There is no workaround.

- CSCef77415

Symptoms: Unconfiguring link-bundling over a GE interface causes a bus error on the RP.

Conditions: This symptom is observed on a Cisco 12000 series that runs a Cisco IOS interim release for Release 12.0(30)S and that is configured with 150 link-bundling subinterfaces, some of which have OSPF established. Note, however, that this caveat is resolved in Release 12.0(30)S.

Workaround: There is no workaround.

- CSCef78098

Symptoms: An Engine 1 or Engine 2 Gigabit Ethernet (GE) line card may stop switching traffic even though the line protocol is up. Pings and routing do not work, and traffic does not go through.

Conditions: This symptom is observed a Cisco 12000 series after error recovery and when the **negotiation auto** command is not configured for the interface of the GE line card.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface of the line card.

- CSCef78846

Symptoms: A Cisco 10000 series that is configured for MLP and that has fragmentation enabled may crash at random times.

Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.0(25)SX6a but may also occur in Release 12.0S.

Workaround: Remove the MLP configuration.

- CSCef79749

Symptoms: APS does not function correctly on a channelized OC-48 ISE line card and the output of the **show aps** command shows that the line card is down.

Conditions: This symptom is observed on a Cisco 12000 series.

Workaround: There is no workaround.

- CSCef80260

Symptoms: IP packets with an IP length that is smaller than 64 bytes and that have the More Fragments (MF) flag set to 1 do not go through a Cisco 12000 series.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(27)S3 or Release 12.0(28)S1 and that is configured with a 2-port OC-48 DPT Engine 4+ ingress line card.

Workaround: There is no workaround.

- CSCef80349

Symptoms: An MPLS traffic engineering (TE) tunnel may not come back up after a link flaps.

Conditions: This symptom is observed when the headend of the TE tunnel is a third-party router that has the **no cspf** command configured for the label switched path (LSP) and when the tunnel midpoint is a Cisco router that runs Cisco IOS Release 12.0(25)S1. The symptom occurs when the link downstream (that is, towards the tailend of the tunnel) on the Cisco router fails because the interface on either side of the link is shut down.

In addition, note that the third-party router does not increment the LSP ID when it receives a message, nor does it send a PathTear message in response to a PathErr message.

Possible Workaround: Use an explicit path on the third-party router but without the **no cspf** command enabled.

- CSCef81501

Symptoms: When L2TPv3 tunnels are scaled and the IP Path MTU Discovery feature is enabled, a memory leak and crash may occur.

Conditions: This symptom is observed when multiple Xconnect statements are applied in conjunction with the IP Path MTU Discovery feature in the pseudowire class.

Workaround: Do not enable the IP Path MTU Discovery feature in an L2TPv3 configuration.

- CSCef81555

Symptoms: The running configuration does not show the correct policing rate if the rate is configured to be larger than 4,200,000,000 bps.

Conditions: This symptom is observed on a Cisco 12000 series that runs an interim release for Cisco IOS Release 12.0(30)S.

Workaround: There is no workaround.

- CSCef83864

Symptoms: A Cisco 10000 series reloads unexpectedly.

Conditions: This symptom is observed when 750 VRFs are configured.

Workaround: There is no workaround.

- CSCef84347

Symptoms: When an input QoS policy is applied on a main interface and subinterface of an Engine 3 ATM line card, the QoS policy works on the main interface but not on the subinterface.

Conditions: This symptom is observed on a Cisco 12000 series that runs an interim release for Cisco IOS Release 12.0(30)S when a QoS policy is applied to a layer-2 VC. Layer-3 VCs work fine. Note that this caveat is resolved in Release 12.0(30)S.

Workaround: There is no workaround.

- CSCef86176

Symptoms: The following CLI commands are missing from a Cisco 12000 series:

```
router(config)#map-class frame-relay r
router(config-map-class)#frame-relay ?
    adaptive-shaping    Adaptive traffic rate adjustment, Default = none
    bc                  Committed burst size (Bc), Default = CIR
    be                  Excess burst size (Be), Default = 0 bits
    cir                 Committed Information Rate (CIR), Default = 56000 bps
    custom-queue-list   VC custom queueing
    fecn-adapt          Enable Traffic Shaping reflection of FECN as BECN
    mincir              Minimum acceptable CIR, Default = 1/2 CIR
```

```
priority-group      VC priority queueing
traffic-rate        VC traffic rate
```

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0S.

Workaround: There is no workaround.

- CSCef87309

Symptoms: A basic back-to-back ping fails on an Engine 4+ line card.

Conditions: This symptom is observed on a Cisco 12000 series that runs the c12kprp-p-mz image of a Cisco IOS interim release for Release 12.0(30)S. However, this caveat is resolved in Release 12.0(30)S.

Workaround: There is no workaround.

- CSCef89192

Symptoms: A self-ping may not function on a Cisco 12000 series and traffic may stop.

Conditions: This symptom is observed on a Cisco 12000 series after you remove and reconfigure a port-channel subinterface.

Workaround: Remove the member interfaces from the channel group and add them again. Doing so enables traffic to resume.

- CSCef89925

Symptoms: IPv4 multicast traffic may be punted to the CPU of the RP, causing a throughput of only 700 pps.

Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of Cisco IOS Release 12.0(30)S.

Workaround: There is no workaround.

- CSCef91030

Symptoms: After the default route is received from a remote PE for a VRF, communication stops for traffic via the default route in this VRF on a Cisco 12000 series that functions as a PE router in an MPLS VPN environment. The packets are switched out of the core MPLS interface untagged as native IPv4 packets instead of with MPLS and BGP labels.

Conditions: This symptom is observed when the traffic is received from VRF interfaces on an Engine 2 line card that is installed in a Cisco 12000 series that functions as a PE router.

The symptom occurs in Release 12.0(27)S2, Release 12.0(27)S3, and interim releases for Cisco IOS Release 12.0(30)S. Other releases may be affected too. The symptom does not occur in Release 12.0(24)S2.

The symptom occurs when the VRF ingress interface is configured on an Engine 2 3-port GE line card or Engine 2 1-port OC-48 POS line card. Other line cards may be affected too. The symptom does not occur when the VRF ingress interface is configured on an Engine 0 4-port OC-3 POS line card or 4-port GE ISE line card.

Workaround: There is no workaround.

- CSCef92153

Symptoms: When a VRF VLAN subinterface punts a packet such as an ARP or ICMP packet to the CPU of the line card, the main interface is unable to process a packet such as ICMP packet that is destined for the main interface. When BGP packets enter and leave via the main interface, a BGP neighbor may go down.

These symptoms do not affect non-VRF subinterfaces, only the main interface. Transit packets that pass through the main interface are not affected.

When a non-VRF VLAN subinterface punts a packet to the CPU of the line card, the main interface may return to normal operational.

Conditions: These symptoms are observed on an Engine 4+ Gigabit Ethernet line card that is installed in a Cisco 12000 series that runs Cisco IOS Release 12.0 (25)S. Engine 2 and Engine 3 line cards are not affected. For the symptoms to occur, all of the following conditions must be present:

- A VRF VLAN subinterface is configured on the Engine 4+ line card.
- The main interface is also used with an IP address assigned to it.
- The VRF VLAN subinterface receives a packet such as an ARP or ICMP packet that is punted to the CPU of the line card.

For the BGP neighbor to go down, in addition to the above-mentioned conditions, the **neighbor ip-address password string** command must be configured.

Workaround: If you must use a VRF VLAN subinterface, create another subinterface for non-VRF communication on the same main interface.

Alternate Workaround: Do not use a VRF VLAN subinterface.

- CSCef94619

Symptoms: A VIP may crash while forwarding packets or a watchdog timeout crash may occur on the VIP during statistics collection.

Conditions: This symptom is observed on a Cisco 7500 series that is configured with an RSP4 and that runs Cisco IOS Release 12.0(26)S4.

Workaround: There is no workaround.

- CSCef96458

Symptoms: The OAM emulation status is displayed incorrectly.

Conditions: This symptom is observed when you enter the **show atm pvc** command.

Workaround: There is no workaround.

- CSCef97533

Symptoms: A Cisco 12000 series may take a relatively long time to boot. This situation may cause traffic loss.

Conditions: This symptom is observed when you cold start a Cisco 12000 series that runs a Cisco IOS interim release for Release 12.0(30)S and that is configured with ISE line cards.

Workaround: There is no workaround.

- CSCef97536

Symptoms: When Multiprotocol Label Switching (MPLS) label distribution protocol (LDP) is configured and you enter the **clear ip route EXEC** command, the MPLS forwarding entries for some of the cleared routing prefixes may become unlabeled.

Conditions: This symptom is observed for prefixes that are connected (with an unspecified nexthop IP address) and that are not locally recognized. This situation may occur in a configuration in which two LDP peers are connected by a point-to-point link that uses PPP encapsulation, and in which both interfaces are configured to use IP addresses with /32 masks.

A list of the affected releases can be found at <http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCEe12379>. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

Possible Workaround: Prevent the symptom from occurring by using a shorter network mask when you configure the interfaces or by using another encapsulation such as HDLC.

When the symptom occurs, restore proper operation by forcing the LDP session that is associated with the link to re-establish itself, or by forcing the LDP session to re-advertise labels for the affected prefixes. The LDP session can be reset by entering the **clear mpls ldp neighbor** command, by administratively disabling and then re-enabling one of the interfaces, or by deconfiguring and then reconfiguring LDP on one of the interfaces. The LDP session can be forced to re-advertise labels by modifying the outbound label filtering configuration. However, this method is complicated and should only be attempted if you are already very familiar with the required procedures, and if the routers do not already have a complicated label filtering configuration in place.

- CSCeg00252

Symptoms: When you enter the **show sec-disk0:** command or the **execute-on slot slot-number command** command on the standby RP, no command output is generated.

Conditions: This symptom is observed on a Cisco 12000 series that has dual RPs and that is configured for RPR, RPR+, or SSO redundancy mode. Note that when you enter the **dir sec-disk0:** command on the standby RP, command output is properly generated.

Workaround: There is no workaround.

- CSCeg01168

Symptoms: Counters that are displayed in the output of the **show interface** commands for an ATM interface of an 8-port OC3 ATM line card show incorrect input packet and byte counts.

Conditions: This symptom is observed on a Cisco 12000 series when the Port Mode Cell Relay Support feature is configured on the ATM interface.

Workaround: There is no workaround.

- CSCeg01543

Symptoms: A Cisco 7500 series VIP may crash when its serial interfaces are part of a Multipoint Frame Relay (MFR) bundle.

Conditions: This symptom is observed when a Frame Relay end-to-end fragment is received on an MFR interface.

Workaround: Administratively shut down the MFR interface or shut down the MFR interface on the other side of the link.

- CSCeg01740

Symptoms: A router crashes when you delete a manual static Xconnect service with L2TPv3 encapsulation.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0S.

Workaround: Do not delete a manual static Xconnect service with L2TPv3 encapsulation.

- CSCeg02511

Symptoms: A Cisco 10000 series may display %CHSTM1-3-STATESYNC error messages, and a buffer leak may occur.

Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.0(27)S2 when a Fast Ethernet interface is configured to use DHCP via the **ip address negotiated** command.

Workaround: Do not configure the **ip address negotiated** command. Rather, configure a specific IP address.

- CSCeg03055

Symptoms: Sampled NetFlow may stop functioning.

Conditions: This symptom is observed on a Cisco 12000 series that is configured with an Engine 4+ 4-port OC-48 line card.

Workaround: Disable and re-enable Sampled NetFlow.

- CSCeg03180

Symptoms: A line card in slot 15 is stuck in the WAITRTRY state.

Conditions: This symptom is observed on a Cisco 12816 that is configured with dual RPs when an RP switchover followed by a CSC switchover occurs.

Workaround: Reload the router.

Alternate Workaround: Power down and power up the router.

- CSCeg03606

Symptoms: Multicast VPN (MVPN) traffic does not resume.

Conditions: This symptom is observed on a Cisco 12000 series that runs a Cisco IOS interim release for Release 12.0(30)S and that functions as a PE router that is configured for MVPN.

Workaround: Enter the **clear ip mroute** command.

- CSCeg06154

Symptoms: A router crashes when you delete an MPLS subinterface by entering the **no interface** command.

Conditions: This symptom is observed when the **mpls ip** command is configured on the same MPLS subinterface. For example, consider a router with the following configuration:

```
interface atm1/0.1 mpls
    mpls ip
```

When you enter the **no interface atm1/0.1 mpls** command, the router crashes.

Workaround: There is no workaround.

- CSCeg06618

Symptoms: A 6-port channelized T3 line card and a 2-port Channelized OC-3 line card may continuously generate the following error message:

```
%LC_CX3-2-PLIM_CPU_CRASHED: PLIM CPU Tofab755 - plim reset
```

Controllers and interfaces do not recover.

Conditions: This symptom is observed on a Cisco 12000 series and occurs because of a problem with the recovery mechanism following a forced reset of the PLIM component of the line card. The symptom is visible only if another problem indirectly triggers a forced reset of the PLIM component.

Workaround: There is no workaround. To recover the affected line card, reload the line card by entering **hw-module slot slot-number reload** command.

- CSCeg07296

Symptoms: When you configure an AToM pseudowire, a memory allocation failure occurs followed by data corruption.

Conditions: This symptom is observed on a Cisco 12000 series.

Workaround: There is no workaround.
- CSCeg09141

Symptoms: Sampled NetFlow stops functioning.

Conditions: This symptom is observed on a Cisco 12000 series that is configured with a 4-port OC-48 line card.

Workaround: Disable and then re-enable Sampled NetFlow.
- CSCeg11421

Symptoms: A Cisco 10720 crashes when you delete an IPv6 ACL.

Conditions: This symptom is observed when you delete the IPv6 ACL during the TurboACL compilation.

Workaround: Wait for the ACL to be fully compiled before you delete it.
- CSCeg13924

Symptoms: When an Engine 0 2-port channelized OC-3 line card comes up after you have reloaded the microcode, the E1 interface and controllers come up and the DLCI for an Xconnect service across an MPLS comes up, but the locally switched DLCI for the Xconnect service is down (the state is “OPER DOWN” and the DLCI is inactive).

Conditions: This symptom is observed on a Cisco 12000 series that runs the k4p-mz image of a Cisco IOS interim release for Release 12.0(30)S. However, this caveat is resolved in Release 12.0(30)S.

Workaround: Bring up the locally switched DLCI by deleting and reconfiguring the **xconnect** command.
- CSCeg16739

Symptoms: A Cisco 10720 crashes when you add and remove a large IPv6 ACL very quickly.

Conditions: This symptom is observed only on a Cisco 10720 that has a large 500-line ACL while the ACL is compiling.

Workaround: Wait until the ACL has compiled before you remove the ACL.
- CSCeg16790

Symptoms: A policy map that causes AAL5 IP to enable the **set precedence 4** command does not function. Note that a policy map that causes ATM to enable the **set mpls experimental imposition** works fine.

Conditions: This symptom is observed on a Cisco 12000 series Engine 2 8-port OC-3 ATM line card when a policy map is configured on a PVC that performs Layer-3 forwarding of AAL5 packets.

Workaround: There is no workaround.
- CSCin67419

Symptoms: An MFR interface that is configured on either an MC-4T+, MC-8TE1+, MC-STM1, or MC-2T3+ may enter up/down state.

Conditions: This symptom is observed when one of the member links of the MFR interface goes down while there is continuous bidirectional 64-byte traffic that uses less than half the bandwidth. The symptom occurs within 20 minutes after the traffic flow has started.

Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the MFR interface.

Alternate Workaround: Reconfigure the MFR interface.

- CSCin73902

Symptoms: When you perform an online insertion and removal (OIR) of a Versatile Interface Processor (VIP) in which an Inverse ATM Multiplexer (IMA) port adapter is installed, the slave Route Switch Processors (RSP) in the router may reload.

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(28)S, that is configured with two RSPs, and that has an IMA group configured.

Workaround: There is no workaround.

- CSCin74180

Symptoms: Spurious memory accesses may occur on a VIP in which one or more channelized port adapters are installed. The CPU utilization may increase to 99 or 100 percent, causing the performance of the VIP to be impacted.

Conditions: These symptoms are observed on a Cisco 7500 series that runs Cisco IOS Release 12.3(6) but may also occur in other releases.

Workaround: There is no workaround.

- CSCin74347

Symptoms: Outbound security ACLs are not applied properly on Cisco 10000 series routers.

Conditions: This symptom is observed on all Cisco IOS Release 12.0 S images that contain the fix for CSCed72686.

Workaround: There is no workaround.

- CSCin75482

Symptoms: A router may hang or crash when PA-MC-8TE1+ or PA-MC-2T3+ interfaces are congested with traffic and a QoS configuration such as shaping is configured on the interfaces.

Conditions: This symptom is observed on a Cisco 7200 series but may also occur on other platforms.

Workaround: Avoid congesting the interfaces.

- CSCin77202

Symptoms: A secondary PRE crashes.

Conditions: This symptom is observed on a Cisco 10000 series when the state of the secondary PRE changes while a switchover is in process.

Workaround: Reload the secondary PRE when it returns to the “Standby Hot” state.

- CSCin77553

Symptoms: A PA-A3-8T1IMA or PA-A3-8E1IMA port adapter that is installed in a Cisco 7xxx series may display an increasing “rx_no_buffer” counter in the output of the **show controllers atm** privileged EXEC command, and some PVCs that are configured on the port adapter may stop receiving traffic.

Conditions: This symptom is observed when there is a high-traffic load on the PA-A3-8T1IMA or PA-A3-8E1IMA port adapter.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the PA-A3-8T1IMA or PA-A3-8E1IMA port adapter, or as an alternate workaround, reset the VIP or FlexWAN.

- CSCin78144

Symptoms: A Simple Network Management Protocol (SNMP) trap message is displayed on the console of a Cisco router. Trap messages may be sent by the router. No other functionality is affected.

Conditions: This symptom is observed on a Cisco 7200 series and Cisco 7500 series that run Cisco IOS Release 12.0(29)S when SNMP is enabled and when an Inverse Multiplexing over ATM (IMA) interface goes up or down.

Workaround: There is no workaround.

- CSCin78324

Symptoms: A Cisco 7200 VXR router may hang.

Conditions: This symptom is observed on a Cisco 7200 VXR router that has a PA-MC-8TE1 and that is configured for IPSec encryption, either via tunnel protection or via a crypto map.

Workaround: Disable IPSec encryption.

- CSCin78325

Symptoms: A serial interface of a PA-MC-8TE1+ continues to process packets even after the interface is placed in the “ADMINDOWN” state. The counters in the output of the **show interfaces serial** command may continue to increment even if the serial interface is shut down.

Conditions: This symptom is observed on a serial interface of a PA-MC-8TE1+ when there is a channel-group configuration for the interface.

Workaround: Remove the channel-group configuration for the interface.

- CSCin79436

Symptoms: A Cisco 12000 series does not fragment IP traffic while switching the traffic into the MPLS core even when the size of the incoming IP packets exceeds the IP MTU of the egress interface. This situation causes the traffic to be dropped on the next hop router.

Conditions: This symptom is observed in Cisco IOS Release 12.0(26)S or a later release when all of the following conditions are present:

- The traffic leaves through an egress interface of an Engine-3 line card (on the MPLS core side).
- The imposed label stack contains only explicit null labels.
- The size of the incoming IP packets exceeds the IP MTU of the egress interface.

Workaround: Ensure that the IP MTU of the egress interface exceeds the maximum size of the incoming IP packets.

- CSCin79486

Symptoms: When you delete a subinterface that is configured with a feature such as MQC, the deletion may not take effect and the console may lock up for a few seconds. This situation may have great impact on a link-bundle interface when you attempt to delete a large number of subinterfaces.

Conditions: This symptom is observed on a Cisco 12000 series that runs an interim release for Cisco IOS Release 12.0(30)S. However, this caveat is resolved in Release 12.0(30)S.

Workaround: There is no workaround.

- CSCin79899

Symptoms: When error recovery is performed on a 3-port Gigabit Ethernet (GE) line card that has port 0 in the shutdown state, the 3-port GE line card stop passing traffic on all ports.

Conditions: This symptom is observed on a Cisco 12410 that runs Cisco IOS Release 12.0(23)S or a later release and that is configured with an Engine 2 3-port line card.

Workaround: Reload the 3-port GE line card and leave port 0 in the up/down state.
- CSCin80221

Symptoms: A Cisco router crashes when you enter the **fsck** command for an ATA flash disk.

Conditions: This symptom is observed when the boot sector of the ATA flash disk is corrupted and when the router runs a release that is listed in the “First Fixed-in Version” field at <http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCed58384>. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

Workaround: Format the disk.
- CSCin82862

Symptoms: Multicast traffic is not switched from a multilink interface on a Cisco 7500 series that is configured for distributed multilink PPP (MLP).

Conditions: This symptom is observed when the router is reloaded or when the multilink interface flaps.

Workaround: Enter the **clear ip mds linecard *** command on the Route/Switch Processor (RSP).
- CSCuk49494

Symptoms: An SSO during an MTU change can create FIA buffer inconsistencies between line cards.

Conditions: This symptom is observed on a Cisco 12000 series.

Workaround: Reapply the MTU change on the new active RP.
- CSCuk51177

Symptoms: You may not be able to make a Telnet connection to a Cisco IOS platform.

Conditions: This symptom is observed when the CNS Exec Agent is used to remotely issue an interactive CLI command.

Workaround: There is no workaround.
- CSCuk51269

Symptoms: Multicast packets such as HSRP and OSPF are not received on a port-channel interface.

Conditions: This symptom is observed when a port-channel interface is configured on a Cisco router, when you reload the router, and when the first member is added to the port-channel interface by entering the **no shutdown** interface configuration command on physical interface.

Workaround: Enter the **do shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the port-channel interface.
- CSCuk52952

Symptoms: An Engine 3 ATM line card may continuously crash.

Conditions: This symptom is observed on a Cisco 12000 series that runs an interim release for Cisco IOS Release 12.0(30)S after you configure IP QoS on an ATM interface of the line card. Note, however, that this caveat is resolved in Release 12.0(30)S.

Workaround: There is no workaround.

TCP/IP Host-Mode Services

- CSCdr11085

Symptoms: A memory leak occurs when you enter the **ip tcp selective-ack** global configuration command on a router. The leak is slow but eventually reduces the available memory on the router and causes the router to reload.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.1(1) but may also occur in other releases.

Workaround: Enter the **no ip tcp selective-ack** global configuration command.

- CSCed78149

A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP “hard” error messages.
2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks.
3. Attacks that use ICMP “source quench” messages.

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml>.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected.

Wide-Area Networking

- CSCeb46007

Symptoms: L2TPv2 tunnels with active PPPoX sessions may go down. When you enter the **vpdn debug error** command, you can see that the LAC or LNS resends L2TP control messages that the other side does not acknowledge.

Conditions: This symptom is observed primarily in scaled environments with more than 10,000 PPPoX sessions over more than 500 L2TP tunnels.

Workaround: There is no workaround.

- CSCee44086

Symptoms: After an RP switchover, a multilink PPP interface cannot forward any traffic.

Conditions: This symptom is observed on a Cisco 7500 series, Cisco 10000 series, and Cisco 12000 series.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected multilink PPP interface.

- CSCee75882

Symptoms: A GEIP+ that is installed in VIP may crash.

Conditions: This symptom is observed on a Cisco 7500 series when the Gigabit Ethernet interface or the interface of its neighbor flaps.

Workaround: Stabilize the flapping interface.

- CSCee80904

Symptoms: The **set fr-fecn-becn** policy-map class configuration command in combination with the **priority** and **bandwidth** policy-map class configuration commands may not function properly.

Conditions: This symptom is observed when you enter the commands through cut-and-paste or through test-scripting.

Workaround: Enter the commands manually.

- CSCef45174

Symptoms: A Cisco router crashes with a SegV exception as soon as a packet is received on a BVI interface.

Conditions: This symptom is observed on a Cisco 2651XM that runs Cisco IOS Release 12.3(9a) and that has IRB configured on an MFR interface. The symptom may be platform-independent and may occur on other platforms in a similar configuration and in other releases.

Workaround: There is no workaround. Note that the symptom does not occur in interim Release 12.3(7.6) and earlier releases.

- CSCef45502

Symptoms: A connection remains to exist on a line card even though the connection is deleted on the RP.

Conditions: This symptom is observed on a Cisco 12000 series when you enter the **no frame-relay interface-dlci** command.

Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the affected interface.

- CSCef58437

Symptoms: The following message is generated when T1s are moved from an MLP bundle to an MFR bundle:

```
%LCINFO-3-CRASH: Line card in slot 3 crashed SLOT X:XX:XX:XX:
%LC_CX3-2-PLIM_CPU_CRASHED: PLIM CPU Frfab755 - plim reset
```

The following message and traceback may also be generated:

```
SLOT X:XX:XX:XX: %LC_DMLP-4-BUNDLENUL: Unexpected null bundle in
bflc_cx3_dmlp_del_link, searching for MFR1
-Traceback= 40309310 4030998C 40E502AC 40E506A0 40E5132C
```

Conditions: This symptom is observed on a Cisco 12000 series that is connected back-to-back to another Cisco 12000 series via 6-port channelized T3 line cards. However, the symptom may not be platform-specific.

Workaround: On both routers, enter the **hw-module slot x reload** command, in which the *x* represents the affected slot in which the 6-port channelized T3 line card is installed.

- CSCef68547

Symptoms: FR links on 6-port channelized T3 and 2-port OC-3-channelized-to-DS1/E1 line cards may not recover when all of the links are removed and reconfigured for an MFR bundle. The same symptom may occur on serial interfaces.

Conditions: This symptom is observed when all links are removed from and re-added to the bundle while the bundle is briefly in a shut down state.

Workaround: To re-establish the bundles, enter the **hw-module slot shelf-id/slot-number reload** command. You can also delete and reconfigure the MFR interface or the serial interfaces. To prevent the symptom from occurring, wait a couple of seconds between entering the **shutdown** command and the **no shutdown** command when you remove and reconfigure the MFR bundle or serial interfaces.

- CSCef77523

Symptoms: The protocol may go down on random Multilink Frame Relay (MFR) link bundles.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S and that is configured with a 1-port channelized OC-12/STM-4 (DS1/E1) ISE line card after you have reloaded the router.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface.

- CSCef82683

Symptoms: An MFR bundle may stay in the down state after redistributing bundle links. The output of the **show frame-relay multilink** command displays as cause code “inconsistent bundle.”

Conditions: This symptom is observed when a Remove-Link message is lost.

Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the affected bundle.

- CSCin05330

Symptoms: When a multilink bundle interface is created by entering the **interface multilink group-name** global configuration command, the Cisco Discovery Protocol (CDP) becomes incorrectly disabled. If the **cdp enable** interface configuration command is used to enable CDP on the multilink bundle interface, the command is not saved in the startup configuration and CDP remains disabled after the router is reloaded.

Conditions: This symptom is observed on a Cisco platform that is configured with a multilink bundle interface.

Workaround: There is no workaround.

- CSCin79140

Symptoms: A router crashes when you apply a map-class configuration to a subinterface that has been unconfigured and reconfigured.

Conditions: This symptom is observed when the following sequence of events occurs:

1. Configure a Frame Relay subinterface.
2. Unconfigure the Frame Relay subinterface.
3. Reconfigure the Frame Relay subinterface.
4. Configure a map class on the subinterface.

Workaround: There is no workaround.

- CSCuk51367

Symptoms: A router may crash if a multipoint Frame Relay subinterface is deleted.

Conditions: This symptom is observed only when there are multiple PVCs configured on the Frame Relay subinterface and when these PVCs have maps attached to the VCs.